Ανάλυση Δικτυακής Κίνησης του Ανώτατου Τεχνολογικού των Χανίων

Πτυχιακή Εργασία

- Λεμπέσης Μάριος
- Κεζούδης Αναστάσιος

Επιβλέπων Καθηγητής

- Καθ. Εφαρμογών Διπλ. Μηχ. (M.Sc.) Λιοδάκης Γεώργιος

Μέσα από πλήθος πληροφοριών και δρομολογημένων πακέτων στο δίκτυο του Τ.Ε.Ι. Χανίων διαπιστώνουμε χόν προβλήματα που προκύπτουν από μετρήσεις που πραγματοποιούνται. Στο σύνολο τους αυτές οι μετρήσεις αποτελούν τις λύσεις στα όποια προβλήματα ζονται.

ΠΕΡΙΕΧΟΜΕΝΑ

Περιεχόμενα

Σκοπός Εργασίας

Με την εργασία αυτή σκοπεύουμε να περιγράψουμε τη γενική αρχή λειτουργίας του δικτύου του τεχνολογικού εκπαιδευτικού ιδρύματος Χανίων, καθώς επίσης και τη ‘’κίνηση’’ που υπάρχει στο δίκτυο. Σχετικά με τον όρο ‘’κίνηση ‘’ θα επεκταθούμε στη συνέχεια αυτού του κεφαλαίου. Η βάση αυτής της εργασίας βρίσκεται στη συνεχόμενη λήψη και ανάλυση κάποιων μετρήσεων που πραγματοποιούνται στο computer room της σχολής. Αυτές οι μετρήσεις έχουν να κάνουν με τη καταγραφή των πρωτοκόλλων που χρησιμοποιούνται περισσότερο, με τις web διευθύνσεις που έχουν τη μεγαλύτερη ζήτηση αλλά και με τη χρήση του bandwidth που κάνουν οι χρήστες μέσω των ιστοσελίδων που χρησιμοποιούνε. Τα αποτελέσματα θα μας δώσουν μια γενική εικόνα της κατάστασης του δικτύου και θα μας δείξουν που εντοπίζονται τα προβλήματα που τυχόν παρουσιάζονται σε αυτό.

Ένας άλλος στόχος της εργασίας είναι να εντοπίσουμε τη βάση των προβλημάτων που υπάρχουν στο δίκτυο και να βγάλουμε ένα συμπέρασμα για το τι ακριβώς επίκειται να συμβεί με τη λειτουργία του Wireless Network της σχολής καθώς επίσης και με την έναρξη χρήσης του νέου κτηρίου. Δεχόμενοι λοιπόν τα οποιαδήποτε προβλήματα προκύψουν από τη μελέτη χρήσης του δικτύου, θα προσπαθήσουμε να δώσουμε πιθανούς τρόπους αντιμετώπισης είτε σε επίπεδο hardware, αυξάνοντας των υπάρχοντα εξοπλισμό, είτε σε επίπεδο software , με τη χρήση δηλαδή κάποιου λογισμικού ελέγχου – ασφαλείας προκειμένου να αντιμετωπιστεί η κακόβουλη χρήση και επιβάρυνση του δικτύου.

Η σύνθεση αυτής της εργασίας περιλαμβάνει επίσης και τα σχέδια του νέου κτηρίου της σχολής υλοποιημένα σε AutoCad 2004 Mechanical σύμφωνα με την ηλεκτρομηχανολογική μελέτη που έχει πραγματοποιηθεί. Βάση αυτών των σχεδίων μπορούν να υπολογιστούν οι θέσεις λειτουργίας ανάλογα με τις ανάγκες της σχολής, επομένως να συμπεράνουμε αν ο υπάρχων εξοπλισμός πληροί τις προϋποθέσεις για σωστή λειτουργία της ενσύρματης και ασύρματης δικτύωσης του εκπαιδευτικού ιδρύματος. Επίσης θα δημοσιευτεί το εγχειρίδιο παραμετροποίησης και εγκατάστασης του ασύρματου δικτύου της σχολής που πραγματοποιήσαμε και συγγράψαμε στα πλαίσια της εργασίας μας στο γραφείο Τηλεπικοινωνιών και Δικτύων του Τ.Ε.Ι. Χανιών.

ΚΕΦΑΛΑΙΟ 1ο

1.1 Εισαγωγή στα δίκτυα

Δίκτυα, μια λέξη με τόσο γενικευμένη έννοια, με μεγάλη και ποικίλη χρήση, τέτοια που πολλές φορές δημιουργούνται ακόμα και παρεξηγήσεις για την ερμηνεία της. Τη λέξη δίκτυο συναντάμε στο ταχυδρομικό δίκτυο, το τηλεφωνικό δίκτυο, το δίκτυο πρατηρίων της ΕΚΟ, στα δίκτυα υπολογιστών, στο τηλεοπτικό δίκτυο, στο δίκτυο καταστημάτων σούπερ μάρκετ, δίκτυο πρακτόρων μυστικών υπηρεσιών κλπ.

Στην περιοχή της τηλεπληροφορικής αναφέρονται τα δημόσια δίκτυα δεδομένων (Hellaspac, Hellascom), το διαδίκτυο, τα στρατιωτικά δίκτυα, τα ιδιωτικά δίκτυα όπως τα τραπεζικά, κλπ.

Οι πρωτόγονες μορφές επικοινωνίας όπως τα σήματα καπνού, οι φωτιές, τα τύμπανα, οι ταχυδρομικές άμαξες κλπ., ούτε ακριβείς ήταν ούτε διέθεταν την βεβαιότητα της επιτυχίας. Παράλληλα η ταχύτητα μεταφοράς της πληροφορίας ήταν αρκετά μικρή, ο όγκος της πληροφορίας ελάχιστος, η δε ασφάλεια της ελάχιστη. Αυτές οι μορφές επικοινωνίας διατήρησαν την αίγλη τους μέχρι την εμφάνιση του ηλεκτρισμού. Ο Samuel Morse το 1845 με τον τηλέγραφο και ο Graham Bell το 1876 με το τηλέφωνο έθεσαν τα θεμέλια μιας νέας εποχής στον κόσμο, μιας εποχής όπου οι τηλεπικοινωνίες θα έπαιζαν βασικό ρόλο στην ανάπτυξη του.

Όταν ο Γκράχαμ Μπέλ έθεσε για πρώτη φορά σε πρακτική εφαρμογή το τηλέφωνο το 1876, συνομιλούσε αυτός με ένα φίλο του μέσω δυο τηλεφωνικών συσκευών και μιας γραμμής. Όταν και άλλοι φίλοι του ζήτησαν να έχουν και αυτοί το ίδιο προνόμιο, ο Μπέλ για κάθε τέτοια σύνδεση διέθετε από δύο τηλεφωνικές συσκευές και από μια γραμμή. Έτσι ο ίδιος που μπορούσε να μιλήσει με όλους, είχε στο σπίτι του τόσες συσκευές όσες και οι συνδέσεις, ενώ παράλληλα ο ίδιος αριθμός γραμμών ξεκινούσε από εκεί με προορισμό τους φίλους του. Όσο ο αριθμός των χρηστών μεγάλωνε, τόσο μεγάλωνε και ο αριθμός των γραμμών και των συσκευών. Η αύξηση ήταν τέτοια ώστε σε λίγο χρονικό διάστημα φάνηκε ότι η κατάσταση αυτή δεν ήταν δυνατόν να συνεχιστεί, καθώς από κάποιο σημείο και μετά το πρόβλημα της πληθώρας θα ήταν άλυτο.

Τότε λοιπόν προέκυψε η ανάγκη του δικτύου. Η λύση του προβλήματος πέρασε τότε πολλά στάδια. Στις αρχές του 20ου αιώνα δημιουργήθηκαν τα πρώτα τηλεφωνικά κέντρα. Την εποχή εκείνη οι τηλεφωνήτριες που χειρίζονταν τα κέντρα (οι

τηλεφωνικές εταιρείες ανακάλυψαν από νωρίς ότι, λόγω ιδιοσυγκρασίας και όχι φυσικά λόγω γνώσεων ή ικανοτήτων, οι γυναίκες είναι μάλλον καταλληλότερες για τηλεφωνήτριες από τους άντρες), ως καλοί τροχονόμοι συνέδεαν την γραμμή του καλούντος συνδρομητή με αυτήν του καλούμενου με την βοήθεια βυσμάτων. Ειδικές γεννήτριες ρεύματος, ενσωματωμένες στις τηλεφωνικές συσκευές, επέτρεπαν τις κλήσεις προς το κέντρο καθώς δεν υπήρχε η πολυτέλεια της επιλογής αριθμού. Αυτή ήταν και η πρώτη μορφή δικτύου επικοινωνιών φωνής. Η τηλεφωνία στην Αμερική ακόμη και πριν τον Πρώτο Παγκόσμιο Πόλεμο αναπτυσσόταν με τόσο ραγδαίο ρυθμό που ήταν φανερό ότι θα οδηγούσε σε αδιέξοδο. Με τους χειροκίνητους τηλεφωνικούς πίνακες, τα δίκτυα πύκνωναν τόσο πολύ που είχε υπολογισθεί ότι πολύ σύντομα θα χρειαζόταν το σύνολο της εργασιακής δύναμης των Η.Π.Α. να μην κάνει τίποτα άλλο παρά να διεκπεραιώνει τηλεφωνικές κλήσεις στους τηλεφωνικούς πίνακες!

Εικόνα 1. Τηλεφωνήτριες στην Βιρτζίνια των Η.Π.Α., στις αρχές της δεκαετίας του 1880.

Ευτυχώς η ανάγκη αυτή βρήκε διέξοδο και ανακούφιση στην ανάπτυξη των ηλεκτρομηχανικών τηλεφωνικών κέντρων και τη χρήση της αυτόματης επιλογής. Στις αρχές τις δεκαετίας του ΄50 άρχισαν να εμφανίζονται τα πρώτα πληροφοριακά συστήματα. Συχνά σχεδιάζονταν και λειτουργούσαν σε απομόνωση το ένα από το άλλο. Η μεταφορά δεδομένων από υπολογιστή σε υπολογιστή δεν ήταν δυνατή, ούτε καν από εφαρμογή σε εφαρμογή. Στα τέλη της δεκαετίας του 1950 χρησιμοποιήθηκαν τηλεφωνικές γραμμές αποκλειστικά για σύνδεση υπολογιστών με απομακρυσμένους υπολογιστές. Ήταν μια πρωτόγονη μορφή αυτού που αργότερα ονομάστηκε “δίκτυο τηλεπληροφορικής”. Ακολούθησαν τα ηλεκτρονικά κέντρα, για να καταλήξουμε σήμερα στα σύγχρονα υπολογιστικά συστήματα, στις ψηφιακές τεχνικές επιλογής και μετάδοσης και την χρήση της ηλεκτρομαγνητικής ακτινοβολίας στις τηλεπικοινωνίες. Δίκτυο τηλεπληροφορικής είναι ένα σύστημα επικοινωνιών το οποίο διαθέτει συσκευές τηλεπικοινωνιών, τηλεπικοινωνιακούς κόμβους, καθώς και τα φυσικά μέσα διέλευσης της πληροφορίας. Πολλές φορές στην προσπάθεια των εταιρειών υπολογιστών να καλύψουν τα

θέματα των τηλεπικοινωνιών, παρατηρείται το φαινόμενο τα σύνορα μεταξύ της πληροφορικής και των τηλεπικοινωνιών να γίνονται δυσδιάκριτα. Γι' αυτό πολλές φορές δεν είναι εύκολος και σαφής ο προσδιορισμός των δικτύων.

Οι κυριότερες απαιτήσεις που καλείται να εκπληρώσει ένα σύγχρονο δίκτυο είναι:

- Ο διαμοιρασμός υπολογιστικών πόρων (προγράμματα, δεδομένα, περιφερειακά).
- Η παροχή υψηλής αξιοπιστίας.
- Η μείωση του κόστους.
- Η επικοινωνία μεταξύ των χρηστών.

Όσο αφορά την πρώτη απαίτηση, τον διαμοιρασμό των υπολογιστικών πόρων, νομίζω ότι λίγο ή πολύ μπορεί ο καθένας να καταλάβει τι περίπου σημαίνει και νομίζω ότι το ίδιο ισχύει και για την τέταρτη απαίτηση γι' αυτό θα αναφερθώ εν συντομία μόνο στις υπόλοιπες:

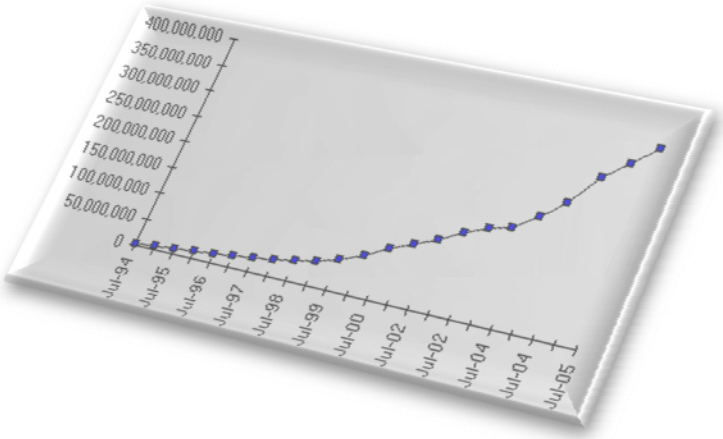
Εικόνα 2. Ο πρώτος μικροϋπολογιστής, Altair 8800. Παρουσιάστηκε επίσημα τον Ιανουάριο του 1975.

➢ Η παροχή υψηλής αξιοπιστίας επιτυγχάνεται κυρίως με τη χρήση εναλλακτικών πηγών υποστήριξης. Για παράδειγμα, είναι δυνατό όλα τα αρχεία να αποθηκεύονται σε δύο ή περισσότερους υπολογιστές. Έτσι, αν παρουσιαστεί βλάβη σε έναν από αυτούς, μπορούν να χρησιμοποιηθούν τα αντίγραφα που βρίσκονται σε έναν άλλο υπολογιστή. Κάθε φορά που ζητάτε μια πληροφορία από π.χ. τον Παγκόσμιο Ιστό (*World Wide Web*) αυτή δεν "μεταφέρεται" στον υπολογιστή σας αλλά στην πραγματικότητα αντιγράφεται.

➢ Η μείωση του κόστους που προσφέρουν τα δίκτυα οφείλεται στο γεγονός ότι οι μικρο-υπολογιστές (*micro-computers*) που έκαναν την πρώτη τους εμφάνιση το 1975 με τον Altair 8800, έχουν πολύ καλύτερο λόγο τιμής προς απόδοση από τους μεγάλους υπολογιστές (*mainframes*), οι οποίοι είναι μάλλον ογκώδεις (περίπου στο μέγεθος που έχει ένα πολυτελές "στούντιο" στο κέντρο της Αθήνας), αλλά λίγο πιο ακριβοί. Επίσης, οι δυνατότητες ενός συστήματος μπορούν να επεκτείνονται

βαθμιαία, καθώς αυξάνονται οι απαιτήσεις, προσθέτοντας απλά περισσότερους επεξεργαστές. Αντίθετα, όταν ένας κεντρικός υπολογιστής φθάσει στο όριο των δυνατοτήτων του, συνήθως πρέπει να αντικατασταθεί ολόκληρος από ένα μεγαλύτερο σύστημα, με πολύ μεγαλύτερο κόστος. Επίσης το κόστος διασύνδεσης των υπολογιστών μειώνεται από την στιγμή που εμφανίστηκαν τα πρώτα τοπικά δίκτυα (*LANs – Local Area Networks*) την δημιουργική δεκαετία του 1970, χαρακτηριστικό δείγμα της οποίας ήταν ο εκσυγχρονισμός και η επέκταση του ARPANET (ο πρόγονος του Internet). Το κόστος διασύνδεσης ενός υπολογιστή σε ένα τοπικό δίκτυο έπεσε από τα 10.000 δολάρια που ήταν το 1980, στα 50 δολάρια ή και λιγότερο μέχρι το τέλος της δεκαετίας του ΄80. Στις αρχές της ίδιας δεκαετίας, η χρήση δορυφόρων μείωσε το κόστος μετάδοσης τηλεφωνικών, υπολογιστικών και τηλεοπτικών σημάτων ανά τον κόσμο. Το κόστος των επικοινωνιών μειώθηκε ακόμη περισσότερο με την έλευση των καλωδίων οπτικών ινών (fiber optic cables) στις αρχές της δεκαετίας του 1990. Κάπου σε αυτό το χρονικό σημείο άρχισαν να συνδέονται στο διαδίκτυο οι μεσαίες και μικρές επιχειρήσεις. Τέλος, τα δίκτυα επιτρέπουν την διατήρηση της επένδυσης μιας επιχείρησης ή ενός οργανισμού στον υπάρχοντα εξοπλισμό. Συχνά επιτρέπουν διασύνδεση διαφορετικών τύπων υπολογιστικών συστημάτων, καλωδίων και περιφερειακών, που χρησιμοποιούν διαφορετικά πρότυπα δικτύων και τεχνολογίες.

Έτσι καλύπτονται καλύτερα οι επιμέρους ανάγκες μιας επιχείρησης, με εξειδικευμένο εξοπλισμό για κάθε περίπτωση, ενώ ταυτόχρονα υπάρχει τάχιστη επικοινωνία και συνεργασία μεταξύ των χρηστών με συνεπακόλουθη αύξηση της παραγωγικότητας. Με την αλματώδη ανάπτυξη της τεχνολογίας σε μέσα μετάδοσης όπως οι οπτικές ίνες, σε ασύρματα δίκτυα, σε τεχνικές μεταγωγής και κόμβους υψηλών ταχυτήτων, δημιουργούνται συνεχώς νέα δίκτυα και υπηρεσίες όπως video on demand, βιντεοτηλεφωνία, επικοινωνίες πολυμέσων κλπ. Η επανάσταση που προμηνύεται στα δίκτυα, είναι η επέκταση των ψηφιακών ασύρματων επικοινωνιών υψηλών ταχυτήτων που επιτρέπουν την πρόσβαση σε φορητά τερματικά πολυμέσων, που θα αλ-



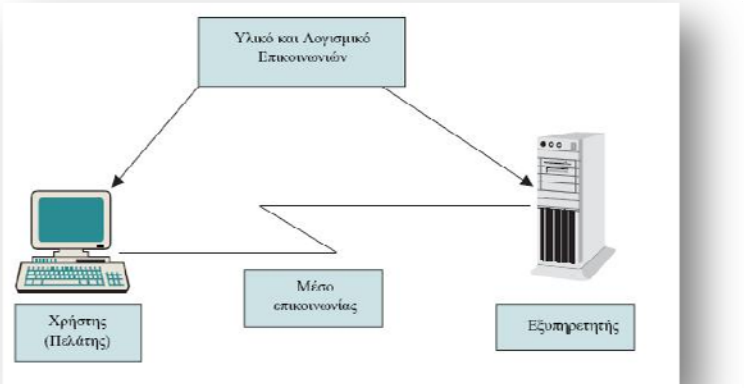
Εικόνα 3. Πλήθος κόμβων συνδεδεμένων στο ,ιαδίκτυο. Πηγή δεδομένων: Internet Software Consortium

λάξει την μορφή των δικτύων καθώς τα σύγχρονα τερματικά σημεία του δικτύου δεν θα εξαρτώνται από το που καταλήγει το καλώδιο, αλλά θα έχουν την ελευθερία κίνησης που προσφέρει η ασύρματη επικοινωνία. Οι σημερινές τεχνολογικές εξελίξεις επιτρέπουν την υπόθεση ότι ο υπολογιστής του μέλλοντος δεν θα είναι παρά ένα στοιχείο του διαδικτύου. Θα παίζει το ρόλο της διασύνδεσης (interface) ανάμεσα στον χρήστη και στο σύνολο των παρεχόμενων από το διαδίκτυο πληροφοριών, με τητα πρόσβασης στην "καθολική βιβλιοθήκη της γνώσης". Το ηλεκτρονικό ταχυδρομείο θα αντικαταστήσει πολλές ταχυδρομικές υπηρεσίες, αφού είναι γελοίο να κόβουμε πολύτιμα δέντρα και να φτιάχνουμε χαρτί για να στέλνουμε μηνύματα από τη μια άκρη της χώρας στην άλλη, όταν αυτά μπορούν να διαβιβαστούν μέσω ενός σύρματος.

Όμως αυτή η προσφερόμενη δυνατότητα όπου ο καθένας με μια φθηνή τερματική συσκευή όπως ένας υπολογιστής, μπορεί να επικοινωνεί με άλλους υπολογιστές, δημιουργεί και μεγάλα προβλήματα. Απαιτείται μεγάλη προσοχή, σαφείς κανόνες, μεγάλη αυστηρότητα και συνεπώς μεγάλη πολυπλοκότητα για να εξασφαλισθεί η με σαφείς όρους συμμετοχή του καθενός σε ένα τέτοιο δίκτυο. Η φύση του ανθρώπινου παράγοντα δεν εξασφαλίζει ότι τα πράγματα θα είναι πάντα έτσι.

1.1.1 Βασικές αρχές δικτύων

Στην πιο απλή του μορφή, ένα δίκτυο αποτελείται από δύο συσκευές, που συνδέονται με κάποιο μέσο, και από υλικό και λογισμικό, που ολοκληρώνει την επικοινωνία. Σε μερικές περιπτώσεις η μία συσκευή είναι υπολογιστής (που μπορεί να ονομάζεται και εξυπηρετητής) και η άλλη είναι μια απλή συσκευή Εισόδου/Εξόδου (που μπορεί να ονομάζεται και πελάτης). Επιπλέον, απαιτείται ακόμη, συνήθως, ένα πληκτρολόγιο για είσοδο και ένας εκτυπωτής για έξοδο.

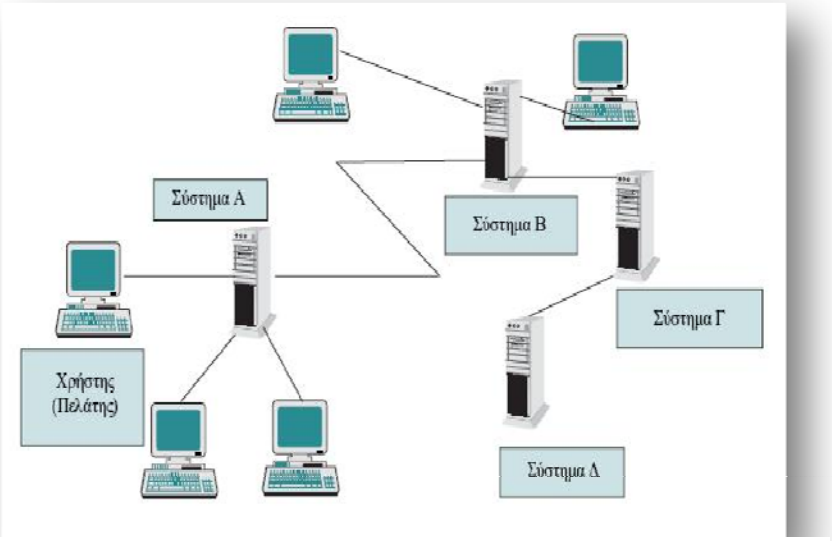


Εικόνα 4. Ένα βασικό δίκτυο

Αν και το μοντέλο αυτό ικανοποιεί τον ορισμό ενός δικτύου, η πραγματικότητα είναι (δυστυχώς) συνήθως πολύ πιο πολύπλοκη.

Πράγματι, η απλή συσκευή Εισόδου/Εξόδου (για τη επικοινωνία χρήστη – μηχανής) είναι συνήθως ένας προσωπικός υπολογιστής ή σταθμός εργασίας. Έτσι, ο πελάτης έχει σημαντικές ικανότητες επεξεργασίας και αποθήκευσης. Επιπλέον, είναι πολύ σπάνιο το δίκτυο να αποτελείται απλώς από ένα μοναδικό πελάτη συνδεμένο με ένα μοναδικό εξυπηρετητή. Αντίθετα, η συνηθισμένη κατάσταση είναι πολλοί πελάτες να αλληλεπιδρούν με πολλούς εξυπηρετητές.

Οι υπηρεσίες του δικτύου παρέχονται συνήθως από πολλές μηχανές. Τα μηνύματα κάθε χρήστη απλώς περνούν από κάποιες απ' αυτές και σταματούν για αλληλεπίδραση μόνο σε κάποιες άλλες. Τέλος, ο τελικός χρήστης συνήθως δε γνωρίζει πολλά από τα μηνύματα και τους υπολογισμούς που στέλνονται ή εκτελούνται για λογαριασμό του.



Εικόνα 5. Ένα πραγματικό δίκτυο

Έτσι, ενώ ένα βασικό δίκτυο μοιάζει μ' αυτό της εικόνας 4, ένα πραγματικό δίκτυο μάλλον μοιάζει περισσότερο μ' αυτό της εικόνας 5.

1.1.2 Στοιχεία δικτύων

Κάθε υπολογιστικό σύστημα σε ένα δίκτυο συνήθως καλείται *κόμβος*, ενώ ο υπολογιστής του καλείται *τελικό σύστημα* (host). Συνδέσεις ανάμεσα σε τελικά συστήματα καλούνται *ζεύξεις*.

Οι χρήστες επικοινωνούν με δικτυωμένα συστήματα μέσω τερματικών, σταθμών εργασίας και υπολογιστών. *Τερματικό* είναι μια απλή συσκευή, ικανή να μεταδίδει και να λαμβάνει σειρές χαρακτήρων. Αν και ένα τερματικό μπορεί να κάνει μικρές εργασίες, όπως εμφάνιση δεδομένων σε συγκεκριμένες θέσεις πάνω στην οθόνη, δεν μπορεί να επιτελέσει πιο πολύπλοκη επεξεργασία δεδομένων. Ο *σταθμός εργασίας* έχει περισσότερη υπολογιστική ισχύ, και ως εκ τούτου είναι ικανός να εκτελέ-

σει πολύπλοκη επεξεργασία δεδομένων, όπως, για παράδειγμα, μετατροπή κωδικοποιημένων δεδομένων σε γραφική μορφή και εμφάνιση στην οθόνη της εικόνας που προκύπτει. Οι σταθμοί εργασίας συνήθως έχουν και τη δυνατότητα αποθήκευσης δεδομένων. *Υπολογιστικό σύστημα* είναι μια συλλογή από υπολογιστές, που πιθανόν περιλαμβάνει τόσο σταθμούς εργασίας όσο και ανεξάρτητους (δηλαδή μη συνδεμένους σε δίκτυο) υπολογιστές, με συνολικά μεγαλύτερη υπολογιστική ισχύ και αποθηκευτική ικανότητα από ένα μεμονωμένο σταθμό εργασίας.

1.1.3 Επικοινωνίες

Όλες οι επικοινωνίες δεδομένων γίνονται είτε σε ψηφιακή μορφή (στην οποία τα δεδομένα εκφράζονται ως διακριτές ψηφιακές τιμές) είτε σε αναλογική μορφή (στην οποία τα δεδομένα εκφράζονται ως σημεία σε μια συνεχή περιοχή τιμών, όπως, π.χ., ένας ήχος ή η τάση του ηλεκτρικού ρεύματος). Οι υπολογιστές συνήθως αποθηκεύουν και επεξεργάζονται ψηφιακά δεδομένα, αλλά πολλά τηλεφωνικά και άλλα ομοειδή ενσύρματα συστήματα επικοινωνίας είναι αναλογικά. Επομένως, ο πομπός πρέπει να μετατρέψει τα ψηφιακά σήματα σε αναλογικά για να μπορέσει να τα μεταδώσει. Αντίστροφα, ο δέκτης πρέπει να τα ξαναμετατρέψει στη αρχική τους ψηφιακή μορφή προκειμένου να μπορέσει να τα επεξεργαστεί. Αυτές οι μετατροπές γίνονται από τους *Διαμορφωτές – Αποδιαμορφωτές*, τα γνωστά Modems, που μετατρέπουν τα ψηφιακά δεδομένα σε αναλογικά σήματα, και αντίστροφα.

Τα συστήματα επικοινωνίας χρησιμοποιούν διάφορα είδη φυσικών μέσων για τη μετάδοση των μηνυμάτων που διαχειρίζονται. Παραδείγματα (τα πιο συνηθισμένα) τέτοιων φυσικών μέσων είναι τα σύρματα και ο αέρας. Ένα σύστημα που χρησιμοποιεί σύρματα στις ζεύξεις του λέμε ότι είναι *σύστημα ενσύρματης επικοινωνίας*. Αντίστοιχα, ένα σύστημα που χρησιμοποιεί άλλο φυσικό μέσο λέμε ότι είναι *σύστημα ασύρματης επικοινωνίας*.

Το πιο συνηθισμένο φυσικό μέσο ενσύρματης επικοινωνίας είναι το απλό καλώδιο. Το μέσο που χρησιμοποιείται πιο συχνά μέσα σε σπίτια και γραφεία είναι ένα ζευγάρι μονωμένων χάλκινων καλωδίων (twisted pair). Ως υλικό, ο χαλκός παρουσιάζει πολύ καλές ιδιότητες αγωγιμότητας, ενώ έχει σχετικά μικρό κόστος. Δυστυχώς, το εύρος ζώνης ενός τέτοιου συστήματος επικοινωνίας είναι μάλλον περιορισμένο, με συνέπεια να μην είναι δυνατή η μετάδοση πολλών μηνυμάτων ταυτόχρονα μέ-

σω μιας και μοναδικής γραμμής. Για το λόγο αυτό, η χρήση του χαλκού περιορίζεται συνήθως σε τοπικό επίπεδο, δηλαδή μέσα σε ένα σπίτι ή γραφείο και μέχρι τον τοπικό κατανεμητή. Το *ομοαξονικό καλώδιο*, επίσης συνηθισμένο φυσικό μέσο ενσύρματης επικοινωνίας, έχει μεγαλύτερο εύρος ζώνης από το χαλκό. Η ποιότητα του σήματος που περνάει μέσα από χάλκινο ή ομοαξονικό καλώδιο μειώνεται με την απόσταση. Για το λόγο αυτό, ανά τακτά διαστήματα, κατά μήκος μιας καλωδιακής σύνδεσης τοποθετούνται *επαναλήπτες*, οι οποίοι λαμβάνουν το σήμα, το ενισχύουν και το αναμεταδίδουν.

Μια νεότερη μορφή καλωδίου είναι η *οπτική ίνα*, που είναι κατασκευασμένη από πολύ λεπτές ίνες γυαλιού. Αντί να μεταφέρουν ηλεκτρική ενέργεια, οι ίνες αυτές μεταφέρουν φως. Το εύρος ζώνης της οπτικής ίνας είναι μεγαλύτερο από αυτό του χάλκινου καλωδίου, ενώ είναι λιγότερο ευαίσθητη σε παρεμβολές, παρουσιάζει λιγότερο έντονα φαινόμενα υπερπήδησης με γειτονικά μέσα μετάδοσης, έχει μικρότερο κόστος και μικρότερο βάρος για το ίδιο μήκος. Είναι, συνεπώς, πολύ καλύτερο μέσο μετάδοσης από το χαλκό, τον οποίο και τείνει να αντικαταστήσει στα σύγχρονα επικοινωνιακά συστήματα.

Περνώντας στη συζήτηση των ασύρματων συστημάτων, σημειώνουμε ότι ασύρματη επικοινωνία μπορεί να επιτευχθεί με πολλές μεθόδους. Ωστόσο, θα περιοριστούμε εδώ στο να αναφερθούμε σύντομα μόνο σε δύο απ' αυτές: μικροκομματικές ζεύξεις και δορυφορικές ζεύξεις. Οι μικροκομματικές ζεύξεις είναι ιδιαίτερα κατάλληλες για επικοινωνίες σε ανοικτούς χώρους και έχουν εύρος ζώνης συγκρίσιμο με εκείνο του ομοαξονικού καλωδίου. Το βασικό πλεονέκτημα μιας τέτοιας ζεύξης είναι ότι η ισχύς του σήματος είναι καλή σε όλη τη διαδρομή, από το σημείο εκπομπής μέχρι το σημείο λήψης, αίροντας έτσι την ανάγκη για τοποθέτηση επαναληπτών.

Ωστόσο, ένα μικροκομματικό σήμα ταξιδεύει ευθύγραμμα. Επομένως, ο πομπός και ο δέκτης πρέπει να βρίσκονται σε οπτική επαφή. Λόγω της καμπυλότητας της Γης, δεν είναι δυνατόν να τοποθετήσουμε πομπό και δέκτη σε απόσταση μεγαλύτερη από περίπου 60 χιλιόμετρα, αν θέλουμε να κρατήσουμε το ύψος των πυλώνων που τους συγκρατούν σε λογικά επίπεδα. Έτσι, η ανάγκη για επαναλήπτες επανεμφανίζεται.

Οι εταιρείες επικοινωνιών χρησιμοποιούν δορυφόρους σε γεωσύγχρονες τροχιές, δηλαδή σε τροχιές συγχρονισμένες με την τροχιά της Γης. Οι δορυφόροι αυτοί, αφού περιστρέφονται με την ίδια ταχύτητα περιστροφής που περιστρέφεται και η Γη, βρίσκονται μονίμως "αγκυροβολημένοι" πάνω από το ίδιο σημείο της γήινης επι-

φάνειας. Αν και το κόστος κατασκευής και εκτόξευσής τους είναι μεγάλο, το κόστος συντήρησής τους είναι πρακτικά μηδενικό. Επιπλέον, η ποιότητα μιας δορυφορικής ζεύξης είναι συνήθως πολύ ανώτερη από την ποιότητα μιας οποιασδήποτε επίγειας ζεύξης. Οι δορυφόροι λειτουργούν ως αφελείς αναμεταδότες: αναμεταδίδουν ό,τι λαμβάνουν.

1.2 Δικτυακές Υπηρεσίες(Πρωτόκολλα)

Οι περισσότεροι από μας, όταν χρησιμοποιούμε ένα επικοινωνιακό σύστημα, δεν έχουμε ιδέα αν το μήνυμά μας μεταφέρεται μέσω χάλκινου καλωδίου, οπτικής ίνας, δορυφόρου, μικροκομματικής ζεύξης ή μέσω κάποιου συνδυασμού αυτών των φυσικών μέσων. Σε πολλές περιπτώσεις μάλιστα, το σημερινό μήνυμά μας μεταφέρεται με διαφορετικό μέσο απ' αυτό που θα μεταφέρει το αυριανό μας. Δημιουργεί άραγε κάποιο πρόβλημα η άγνοια αυτή; Ασφαλώς όχι. Φανταστείτε τη δυσκολία που θα εμφάνιζε για τους χρήστες του ένα τηλεφωνικό σύστημα που θα απαιτούσε απ' αυτούς να καθορίσουν το φυσικό μέσο της ζεύξης που θέλουν να χρησιμοποιήσουν και, βέβαια, να διαμορφώσουν τα μηνύματά τους αντίστοιχα με την επιλογή τους αυτή. Είναι φανερό ότι κανείς δε θα ήθελε να χρησιμοποιήσει ποτέ ένα τέτοιο σύστημα. Αντίθετα, η (σκόπιμη και επιθυμητή) άγνοια του χρήστη σε οτιδήποτε σχετικό με το φυσικό μέσο επικοινωνίας αποτελεί απόδειξη της ανεξαρτησίας που υπάρχει (και που θέλουμε να υπάρχει) μεταξύ του μηνύματος και του φυσικού μέσου μεταφοράς του. Η ανεξαρτησία αυτή καθίσταται δυνατή χάρη σε *πρωτόκολλα*, που επιτρέπουν στο χρήστη ενός επικοινωνιακού συστήματος να σκέφτεται και να λειτουργεί αφαιρετικά στα υψηλά επίπεδα της επικοινωνίας, αφήνοντας τις λεπτομέρειες της αποστολής του μηνύματός του σε υλικό και λογισμικό που είναι εγκατεστημένο στα δύο άκρα της ζεύξης. Το υλικό και το λογισμικό αυτό σχηματίζουν μια οικογένεια πρωτοκόλλων, που οδηγεί σε μια αρχιτεκτονική επικοινωνιών δομημένη σε επάλληλα διακριτά στρώματα.

Δύο δημοφιλείς οικογένειες πρωτοκόλλων είναι η οικογένεια Open Systems Interconnection (OSI) και η οικογένεια TCP/IP (Transport Control Protocol/Internet Protocol).

1.2.1 Το μοντέλο αναφοράς OSI

Ο Διεθνής Οργανισμός Προτυποποίησης (International Standards Organization – ISO) έχει δημιουργήσει το μοντέλο αναφοράς OSI, το οποίο ορίζει επίπεδα στην αρχιτεκτονική συστημάτων μέσω των οποίων πραγματοποιούνται δικτυακές επικοινωνίες. Το μοντέλο, που ορίζεται στο πρότυπο ISO 7498 και στην οδηγία CCITT X.200, αποτελείται από επτά επίπεδα (ή στρώματα), που φαίνονται στο Σχήμα 2.3.

Κάθε επίπεδο N χρησιμοποιεί τις υπηρεσίες που παρέχονται από το αμέσως

Επίπεδο	Μονάδα δεδομένων
7. Επίπεδο εφαρμογής	Μήνυμα
6. Επίπεδο παρουσίασης	Μήνυμα
5. Επίπεδο συνόδου	Μήνυμα
4. Επίπεδο μεταφοράς	Μήνυμα
3. Επίπεδο δικτύου	Πακέτο
2. Επίπεδο ζεύξης δεδομένων	Πλαίσιο
1. Φυσικό επίπεδο	Bit

Εικόνα 6. Επίπεδα OSI

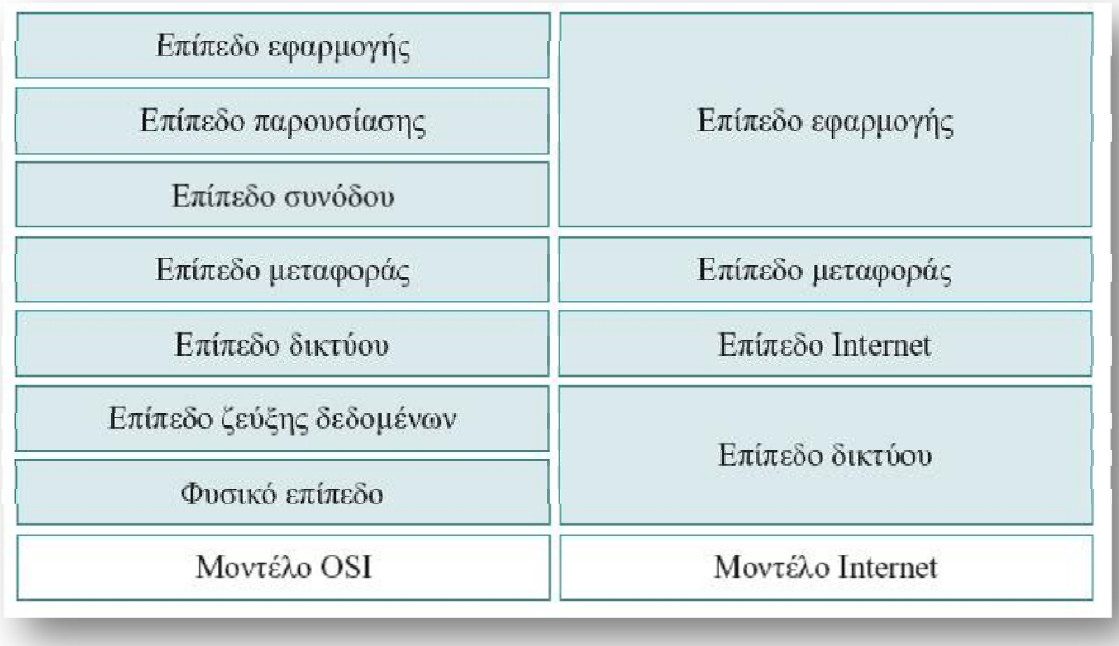
κατώτερο επίπεδο N–1 και τις ενισχύει, προκειμένου να παραγάγει μια πιο ολοκληρωμένη υπηρεσία στο αμέσως ανώτερο επίπεδο N+1. Είναι φανερό ότι, αφού κάθε επίπεδο χρησιμοποιεί άμεσα τις υπηρεσίες τού αμέσως κατωτέρου του, χρησιμοποιεί έμμεσα τις υπηρεσίες και όλων των κατωτέρων του επιπέδων. Το επίπεδο N υλοποιείται από δύο (ή και περισσότερες) επικοινωνούσες οντότητες επιπέδου N (Οντότητες N), οι οποίες ανταλλάσσουν εντολές και δεδομένα μέσω ενός πρωτοκόλλου επιπέδου N (Πρωτοκόλλου N). Οι οντότητες αυτές ενεργοποιούν τις υπηρεσίες του επιπέδου N–1, όπως αυτές παρέχονται σε τοπικές εσωτερικές διεπαφές, για να μεταφέρουν η μία στην άλλη τις μονάδες δεδομένων πρωτοκόλλου (Protocol Data Units – PDUs) επιπέδου N. Οι οντότητες N στη συνέχεια προσφέρουν την ολοκληρωμένη υπηρεσία στο επίπεδο N+1 μέσω εσωτερικών διεπαφών. Η διαδικασία αυτή φαίνεται στο Σχήμα 2.4. Οι υπηρεσίες που προσφέρει κάθε επίπεδο κατατάσσονται σε δύο κατηγορίες:

- σε υπηρεσίες προσανατολισμένες σε σύνδεση, η παροχή των οποίων προαπαιτεί την εγκατάσταση μιας σταθερής σύνδεσης μεταξύ των δύο οντοτήτων που επικοινωνούν, τη διατήρησή της για όσο χρονικό διάστημα διαρκεί η επικοινωνία και τον τερματισμό της μόλις η επικοινωνία ολοκληρωθεί, και

- σε υπηρεσίες χωρίς σύνδεση, η παροχή των οποίων δεν απαιτεί την εγκατάσταση σύνδεσης. Στην περίπτωση αυτή κάθε μήνυμα μεταξύ των οντοτήτων που εμπλέκονται στην επικοινωνία μεταδίδεται αυτόνομα και ανεξάρτητα από κάθε άλλο, ενώ δεν τηρείται απαραίτητα η σειρά διαδοχής των μηνυμάτων κατά τη μετάδοση.

1.2.2 Το μοντέλο αναφοράς TCP/IP

Στην ενότητα αυτή θα κάνουμε μια σύντομη ανασκόπηση του μοντέλου του Internet. Όπως φαίνεται στη δεξιά πλευρά της εικόνας 7, το μοντέλο του Internet αποτελείται από τέσσερα επίπεδα, και συγκεκριμένα το επίπεδο *δικτύου* (ή *προσπέλασης δικτύου*), το επίπεδο *Internet*, το επίπεδο *μεταφοράς* και το επίπεδο *εφαρμογής*. Η διάταξη αυτή είναι κάπως διαφορετική απ' αυτήν του μοντέλου αναφοράς OSI. Ωστόσο, δεν πρέπει να δίνεται και μεγάλη σημασία στο γεγονός αυτό, που οφείλεται κυρίως στο ότι το μοντέλο Internet σχεδιάστηκε πριν από το μοντέλο OSI.



Εικόνα 7. Μοντέλο OSI – Μοντέλο Internet

1.2.2.1 Το επίπεδο προσπέλασης δικτύου

Μέρος της δημοτικότητας της σειράς πρωτοκόλλων TCP/IP οφείλεται στην ικανότητά τους να υλοποιούνται πάνω από διάφορες τεχνολογίες δικτύων και τα αντίστοιχα πρωτόκολλα προσπέλασης δικτύων, όπως τα Ethernet, IEEE 802.3, IEEE 802.4 (Token Bus) και IEEE 802.5 (Token Ring). Η κυρίαρχη στρατηγική σήμερα είναι η χρήση Ethernet για τοπική δικτύωση και η σύνδεση του Ethernet, μέσω μιας γραμμής T1, σε ένα περιφερειακό δίκτυο κορμού TCP/IP, που με τη σειρά του συνδέεται στο Internet. Ο βασικός λόγος που διαμόρφωσε τη στρατηγική αυτή ως κυρίαρχη είναι ότι όλοι οι σημαντικοί προμηθευτές συστημάτων Unix πωλούν τα συστήματά τους με ενσωματωμένη διεπαφή Ethernet. Οι ταχύτητες των modems βελτιώνονται συνεχώς, καθώς εγκρίνονται νέα τηλεπικοινωνιακά πρότυπα, αυξάνοντας έτσι τη δημοτικότητα των μορφών του TCP/IP που λειτουργούν πάνω από το δημόσιο επιλεγόμενο τηλεφωνικό δίκτυο (Public Switched Telephone Network – PSTN). Έτσι, πολλοί χρησιμοποιούν σήμερα το Point–to–Point Protocol (PPP) ή το Serial Line IP (SLIP) για να συνδέσουν τα συστήματά τους σε δίκτυα TCP/IP μέσω του PSTN. Στην περίπτωση αυτή μπορούν να χρησιμοποιήσουν είτε το Password Authentication Protocol (PAP) είτε το CHallenge–response Authentication Protocol (CHAP) για να αυθεντικοποιηθούν.

1.2.2.2 Το επίπεδο Internet

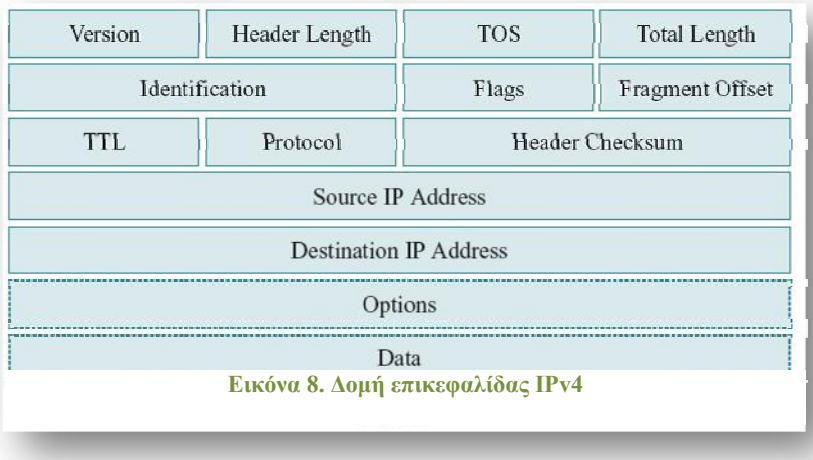
Το Internet Protocol

Το Internet Protocol (IP) είναι το βασικό πρωτόκολλο της οικογένειας TCP/IP. Η τρέχουσα έκδοση του IP είναι η IPv4. Ο χώρος διευθύνσεων της έκδοσης αυτής έχει εύρος 4 bytes. Οι αντίστοιχες διευθύνσεις IP γράφονται συνήθως σε μορφή δεκαδικού με υποδιαστολή, όπου κάθε byte εμφανίζεται ως δεκαδικός αριθμός, τα δε bytes χωρίζονται με τη δεκαδική τελεία και εμφανίζονται σε σειρά από το byte υψηλής τάξης προς το byte χαμηλής τάξης. Κυρίως για να απλοποιηθεί η δρομολόγηση, μια διεύθυνση IP χωρίζεται σε διεύθυνση δικτύου και σε διεύθυνση συστήματος. Για να επικοινωνούν κανονικά όλες οι μηχανές, κάθε διεπαφή δικτύου στο ίδιο τμήμα φυσικού δικτύου πρέπει να έχει την ίδια διεύθυνση δικτύου και μια μοναδική διεύθυνση συστήματος. Αρχικά το IP χρησιμοποιούσε το byte υψηλής τάξης ως διεύθυνση δικτύου και τα τρία bytes χαμηλής τάξης ως διεύθυνση συστήματος. Αλλά, πολύ σύντομα, μετά την διευθέτηση αυτή έγινε φανερό ότι το πλήθος των διασυνδεμένων

δικτύων θα ξεπερνούσε κατά πολύ τα 254. Για να λυθεί λοιπόν το πρόβλημα αυτό, συμφωνήθηκε μια συγκεκριμένη κωδικοποίηση των bits υψηλής τάξης του byte υψηλής τάξης της διεύθυνσης IP, που επιτρέπει στη διεύθυνση δικτύου να έχει μήκος 1, 2 ή 3 bytes, ενώ τα υπόλοιπα χρησιμοποιούνται για διεύθυνση συστήματος. Το σχήμα αυτό κωδικοποίησης χωρίζει το χώρο διευθύνσεων IP σε πέντε κλάσεις διευθύνσεων, που ονοματίζονται ως A, B, C, D και E. Οι κλάσεις A–C είναι οι συνηθέστερα χρησιμοποιούμενες κλάσεις, ενώ η κλάση D είναι δεσμευμένη για διευθύνσεις multicast και η κλάση E για μελλοντική χρήση, εκτός από τη διεύθυνση (255.255.255.255), η οποία μπορεί να χρησιμοποιηθεί μόνον ως διεύθυνση προορισμού και υποδηλώνει όλα τα συστήματα που βρίσκονται στο ίδιο τμήμα φυσικού δικτύου με τον αποστολέα.

Το IP πακετάρει μηνύματα δημιουργώντας ένα πακέτο IP για κάθε μήνυμα που λαμβάνει από κάποιο υποσύστημα πρωτοκόλλου επιπέδου μεταφοράς. Κάθε πακέτο αποτελείται από την επικεφαλίδα IP, η οποία ακολουθείται από το σώμα που μπορεί να περιέχει δεδομένα επιπέδου μεταφοράς. Όσον αφορά το IP, το σώμα είναι απλώς μια σειρά από bytes δεδομένων. Η δομή μιας επικεφαλίδας IPv4 φαίνεται στην Εικόνα 8.

Το πεδίο *Version* (μήκους 4 bits) χρησιμοποιείται για να δηλώσει την έκδοση του IP. Το πεδίο *Header Length* (μήκους 4 bits) περιέχει το μήκος της επικεφαλίδας IP. Το ελάχιστο (και πιο συνηθισμένο) μήκος της επικεφαλίδας είναι 20 bytes. Στην περίπτωση αυτή το συγκεκριμένο πεδίο περιέχει τον αριθμό 5, αφού το μήκος της επικεφαλίδας πρέπει να είναι ακέραιο πολλαπλάσιο λέξεων μήκους 32 bits. Το πεδίο *TOS* (μήκους 8 bits) περιέχει τον τύπο υπηρεσίας (Type Of Service) ή την προτεραιότητα του πακέτου IP. Συνήθως, το πεδίο περιέχει την τιμή 0. Το πεδίο *Total Length* (μήκους 16 bits) περιέχει το συνολικό μήκος του πακέτου (συμπεριλαμβανομένης της επικεφαλίδας) σε bytes. Τα πεδία *Identification* (μήκους 16 bits), *Flags* (μήκους 3 bits) και *Fragment Offset* (μήκους 13 bits) χρησιμοποιούνται για να τεμα-



Εικόνα 8. Δομή επικεφαλίδας IPv4

χίζουν και να ανασυγκροτούν ορθά τα πακέτα IP. Το πεδίο *TTL* (μήκους 8 bits) περιέχει την τιμή του απομένοντος χρόνου ζωής (Time To Live) του πακέτου σε δευτερόλεπτα. Η τιμή αυτή ελαττώνεται κατά τουλάχιστον ένα κάθε φορά που το πακέτο υφίσταται επεξεργασία από κάποιο δρομολογητή ή κεντρικό υπολογιστή. Το πεδίο *Protocol* (μήκους 8 bits) περιέχει έναν κωδικό αναγνώρισης του πρωτοκόλλου των δεδομένων που είναι ενσωματωμένα στο πακέτο IP. Για παράδειγμα, η τιμή του πεδίου αυτού είναι 1 για το ICMP, 6 για το TCP και 17 για το UDP. Το πεδίο *Header Checksum* (μήκους 16 bits) χρησιμοποιείται για ανίχνευση λαθών. Περιέχει το συμπλήρωμα ως προς 1 του αθροίσματος όλων των λέξεων μήκους 16 bits της επικεφαλίδας. Το πεδίο *Source IP Address* (μήκους 32 bits) περιέχει τη διεύθυνση IP προέλευσης του πακέτου. Το πεδίο *Destination IP Address* (μήκους 32 bits) περιέχει τη διεύθυνση IP προορισμού του πακέτου. Το πεδίο *Options* μπορεί να χρησιμοποιηθεί προαιρετικά για:

- επιλογή συγκεκριμένου δρομολογίου,
- καταγραφή δρομολογίου,
- χρονοσφράγιση σε κάθε ενδιάμεσο δρομολογητή,
- ασφάλεια,
- συμπλήρωση της επικεφαλίδας σε άρτιο πολλαπλάσιο των 4 bytes.

Η δουλειά του IP δεν τελειώνει με τη δημιουργία του πακέτου. Πρέπει επίσης να καθορίσει ποια διεπαφή δικτύου πρέπει να χρησιμοποιηθεί και μετά να μεταβιβάσει αρκετή πληροφορία στο υποσύστημα πρωτοκόλλου επιπέδου προσπέλασης δικτύου, ώστε αυτό να μπορέσει κατάλληλα να εσωκλείσει το πακέτο IP στο αντίστοιχο πλαίσιο.

Το IP next generation (IPng) ή έκδοση 6 του IP (IPv6) είναι η νέα έκδοση του IP, που βασίζεται πάνω στην ίδια επιτυχημένη αρχιτεκτονική του IPv4, αλλά σχεδιάστηκε ώστε να αντιμετωπίσει τα προβλήματα ανάπτυξης που αντιμετωπίζει το Internet. Αυτά περιλαμβάνουν τα άμεσα προβλήματα διευθυνσιοδότησης και δρομολόγησης, αλλά και τα μακροπρόθεσμα προβλήματα ανάπτυξης, όπως ασφάλεια, αυτοκαθορισμός και υπηρεσίες πραγματικού χρόνου. Η κύρια διαφορά του IPv6 από το IPv4 είναι η αύξηση του μήκους της διεύθυνσης IP από 32 σε 128 bits. Επιπλέον, κάποια από τα πεδία της IP επικεφαλίδας έχουν καταργηθεί ή έγιναν προαιρετικά, ώστε να ελαττωθεί το κόστος χειρισμού πακέτου στις περισσότερες περιπτώσεις και να περιοριστεί ανάλογα το κόστος εύρους ζώνης της επικεφαλίδας του IPv6.Η εικόνα 9 δείχνει τη δομή μιας βασικής επικεφαλίδας IPv6.

Το πεδίο *Version* (μήκους 4 bits) χρησιμοποιείται, όπως και στο IPv4, για να δηλώσει την έκδοση του IP. Το πεδίο *Priority* (μήκους 4 bits) δηλώνει τη (σχετική) προτεραιότητα του πακέτου IP ως προς άλλα πακέτα που ταξιδεύουν στο δίκτυο. Το πεδίο *Flow Label* (μήκους 24 bits) περιέχει μια τιμή που, μαζί με τη διεύθυνση IP προέλευσης, καθορίζει μια συγκεκριμένη ροή κυκλοφορίας στο δίκτυο. Το πεδίο *Payload Length* (μήκους 16 bits) περιέχει το συνολικό μήκος του πακέτου (μη συμπεριλαμβανομένης της επικεφαλίδας) σε bytes. Το πεδίο *Next Header* (μήκους 8 bits) παίρνει τιμές ανάλογες του πεδίου *Protocol* του IPv4. Το πεδίο *Hop Limit* (μήκους 8 bits) περιέχει το μέγιστο πλήθος επιτρεπόμενων ενδιάμεσων κόμβων. Η τιμή αυτή ελαττώνεται κατά 1 κάθε φορά που το πακέτο περνάει από ενδιάμεσο κόμβο. Αν η τιμή μηδενιστεί, το πακέτο απορρίπτεται. Το πεδίο *Source IP Address* (μήκους 128 bits) περιέχει τη διεύθυνση IP προέλευσης του πακέτου. Το πεδίο *Destination IP Address* (μήκους 128 bits) περιέχει τη διεύθυνση IP προορισμού του πακέτου.

Εικόνα 9. Δομή επικεφαλίδας IPv6

Στο IPv6 προαιρετικές πληροφορίες του επιπέδου Internet μπορούν να τοποθετηθούν σε ξεχωριστές επικεφαλίδες επέκτασης, που τοποθετούνται μεταξύ της βασικής επικεφαλίδας IPv6 και της επικεφαλίδας του πρωτοκόλλου του επόμενου υψηλότερου επιπέδου. Υπάρχει ένας σχετικά μικρός αριθμός τέτοιων επικεφαλίδων επέκτασης, η καθεμιά από τις οποίες αναγνωρίζεται από μια μοναδική τιμή επόμενης επικεφαλίδας. Υπάρχουν καθορισμένες επικεφαλίδες επέκτασης για επιλογές Hop–By–Hop, για δρομολόγηση, για κατακερμάτιση, επιλογές προορισμού, αυθεντικοποίηση και σώμα με ενσωματωμένη ασφάλεια.

Πρωτόκολλα Δρομολόγησης

Ο σκοπός ενός πρωτοκόλλου δρομολόγησης είναι να επιτρέπει τη λήψη αποφάσεων δρομολόγησης στο επίπεδο Internet. Επομένως, το πρωτόκολλο δρομο-

λόγησης πρέπει να διαχειρίζεται και περιοδικά να ενημερώνει τους πίνακες δρομολόγησης που είναι αποθηκευμένοι σε κάθε δρομολογητή. Κάθε δρομολογητής Internet μπορεί να είναι μέρος ενός αυτόνομου συστήματος δρομολόγησης, που είναι βασικά ένα σύνολο δρομολογητών με ενιαία διαχείριση. Οι δρομολογητές αυτοί τρέχουν το ίδιο πρωτόκολλο δρομολόγησης, που συνήθως λέγεται *πρωτόκολλο εσωτερικού πύλης* (Interior Gateway Protocol – IGP). Υπάρχουν διάφορα IGP σε χρήση σήμερα, αλλά όλοι οι δρομολογητές μέσα σ' ένα αυτόνομο σύστημα κανονικά τρέχουν το ίδιο. Ωστόσο, για να επικοινωνήσει με ένα άλλο αυτόνομο σύστημα, ο δρομολογητής συνήθως χρησιμοποιεί ένα *πρωτόκολλο εξωτερικής πύλης* (Exterior Gateway Protocol – EGP). Το EGP δεν γνωρίζει τις λεπτομέρειες της δρομολόγησης στο εσωτερικό μιας άλλης περιοχής δικτύου. Αναλογικά μιλώντας, το IGP είναι το αντίστοιχο του τοπικού τηλεφωνικού κέντρου, ενώ το EGP είναι η τηλεφωνήτρια υπεραστικών.

Σήμερα χρησιμοποιούνται πολλά πρωτόκολλα δρομολόγησης στο Internet, που κατηγοριοποιούνται σε *πρωτόκολλα επισκεψιμότητας* και σε *πρωτόκολλα διανύσματος απόστασης*. Τα πρωτόκολλα επισκεψιμότητας καθορίζουν αν υπάρχει διαδρομή προς κάποιο απόμακρο δίκτυο, ενώ τα πρωτόκολλα διανύσματος απόστασης υπολογίζουν ένα μετρικό της απόστασης προς το απόμακρο δίκτυο. Το μετρικό αυτό μπορεί να είναι απλώς το πλήθος των δρομολογητών μεταξύ των δικτύων προέλευσης και προορισμού ή μπορεί να συμπεριλαμβάνει περισσότερη πληροφορία για κάθε κόμβο, όπως εύρος ζώνης και φορτίο. Γενικά, τα IGP είναι πρωτόκολλα διανύσματος απόστασης και τα EGP πρωτόκολλα επισκεψιμότητας.

Πρωτόκολλα Υποστήριξης

Πρωτόκολλα υποστήριξης του IP χειρίζονται συγκεκριμένες εργασίες, όπως αναδρομολογήσεις, μηνύματα λάθους, και αντιστοιχίσεις μεταξύ διευθύνσεων IP και φυσικών διευθύνσεων επιπέδου προσπέλασης δικτύου. Δεν παίρνουν αποφάσεις δρομολόγησης στο επίπεδο Internet, αν και μπορούν να χρησιμοποιηθούν από πρωτόκολλα που παίρνουν τέτοιες αποφάσεις.

Το πρωτόκολλο *Internet Message Control Protocol* (IMCP) είναι ένα πρωτόκολλο που πρέπει απαραίτητα να υλοποιηθεί μαζί με το IP. Ο σκοπός του είναι να στέλνει πληροφορίες και μηνύματα ελέγχου μεταξύ συστημάτων, όπως μηνύματα λάθους, όταν γίνει προσπάθεια αποστολής πακέτων σε μη επισκέψιμο σύστημα ή δίκτυο, και άλλα μη διορθώσιμα λάθη δρομολόγησης. Τα μηνύματα IMCP στέλνονται ως

δεδομένα πρωτοκόλλου επιπέδου μεταφοράς, δηλαδή ενσωματώνονται σε πακέτα IP. Δοθείσης μιας διεύθυνσης IP, ο σκοπός του πρωτοκόλλου *Address Resolution Protocol* (ARP) είναι να βρει την αντίστοιχη διεύθυνση επιπέδου προσπέλασης δικτύου, ανακοινώνοντας στο τμήμα τοπικού δικτύου ένα μήνυμα που περιέχει τη διεύθυνση IP και αναμένοντας απάντηση. Μόλις δοθεί μια απάντηση ARP για μια διεύθυνση IP, το ζεύγος αυτό διευθύνσεων αποθηκεύεται, ώστε να μη χρειάζεται να υποβληθεί η αίτηση πάλι, τουλάχιστον για κάποιο χρονικό διάστημα. Το ARP συνήθως χρησιμοποιείται πάνω από πρωτόκολλα επιπέδου προσπέλασης δικτύου που υποστηρίζουνανακοινώσεις, όπως το Ethernet.

Δοθείσης μιας φυσικής διεύθυνσης επιπέδου προσπέλασης δικτύου, ο σκοπός του πρωτοκόλλου *Reverse Address Resolution Protocol* (RARP) είναι να βρει την αντίστοιχη διεύθυνση IP. Το RARP είναι ιδιαίτερα χρήσιμο σε σταθμούς εργασίας χωρίς δίσκο, που πρέπει να βρουν μια διεύθυνση IP κατά την εκκίνησή τους.

Τα πρωτόκολλα υποστήριξης είναι πολύ σημαντικά για την ασφάλεια της υλοποίησης του TCP/IP. Για παράδειγμα, μηνύματα αναδρομολόγησης του ICMP μπορούν να χρησιμοποιηθούν για να παραπλανήσουν δρομολογητές και συστήματα που δρουν ως δρομολογητές, ώστε να χρησιμοποιήσουν πλαστά δρομολόγια. Τα δρομολόγια αυτά θα μπορούσαν να βοηθήσουν στο να κατευθύνουν πακέτα προς το σύστημα του επιτιθέμενου αντί για το νόμιμο προορισμό τους.

1.2.2.3 Το επίπεδο μεταφοράς

Τα δύο βασικά πρωτόκολλα επιπέδου μεταφοράς, το TCP και το UDP, συνθέτουν μηνύματα που προέρχονται από διεργασίες εφαρμογής και τα παραδίδουν χρησιμοποιώντας την υπηρεσία παράδοσης πακέτων IP. Επειδή το IP παραδίδει πακέτα μόνο σε συστήματα, τα πρωτόκολλα επιπέδου μεταφοράς πρέπει να προσθέσουν πληροφορίες που θα επιτρέψουν την παράδοση σε διεργασίες εφαρμογής.

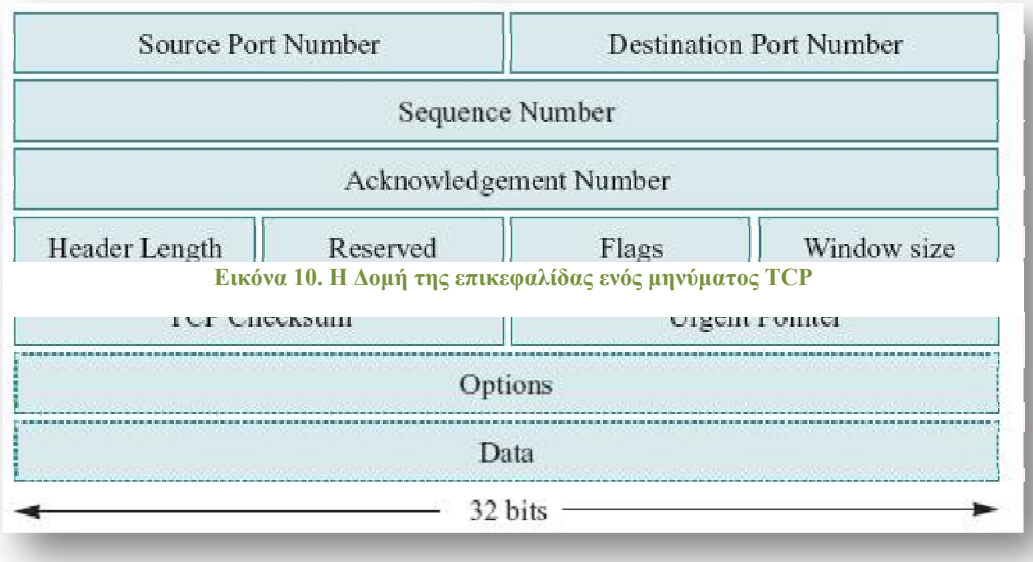
Πρωτόκολλο TCP

Το πρωτόκολλο *Transmission Control Protocol* (TCP) είναι το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο επιπέδου μεταφοράς στο Internet. Παρέχει υπηρεσίες μεταφοράς προσανατολισμένες σε σύνδεση, αξιόπιστες και διπλής κατεύθυνσης, εξα-

λείφοντας έτσι τα διπλά πακέτα, επιτρέποντας το χειρισμό της αναμετάδοσης χαμένων πακέτων και εξασφαλίζοντας ότι τα πακέτα θα παραδοθούν με τη σωστή σειρά. Επειδή παρέχει υπηρεσία μεταφοράς προσανατολισμένη σε σύνδεση, το TCP υλοποιεί εικονικά κυκλώματα μεταξύ των οντοτήτων που επικοινωνούν.

Το υποσύστημα TCP στην προέλευση της σύνδεσης επεξεργάζεται μια ακολουθία bytes από μια διεργασία εφαρμογής και τη διαιρεί σε διακριτά μηνύματα που στέλνονται στο υποσύστημα TCP του προορισμού. Το υποσύστημα TCP του προορισμού, με τη σειρά του, συλλέγει τα μηνύματα, ανακατασκευάζει την αρχική ακολουθία bytes και την περνάει στην αντίστοιχη διεργασία εφαρμογής. Η εικόνα 10 δείχνει τη δομή της επικεφαλίδας ενός μηνύματος TCP.

Τα πεδία *Source Port Number* (μήκους 16 bits) και *Destination Port Number* (μήκους 16 bits), μαζί με τις διευθύνσεις IP προέλευσης και προορισμού που υπάρχουν στην επικεφαλίδα του πακέτου IP, καθορίζουν μοναδικά τις δύο εφαρμογές που σχετίζονται με τη σύνδεση TCP/IP. Το πεδίο *Sequence Number* (μήκους 32 bits) πε-



Εικόνα 10. Η Δομή της επικεφαλίδας ενός μηνύματος TCP

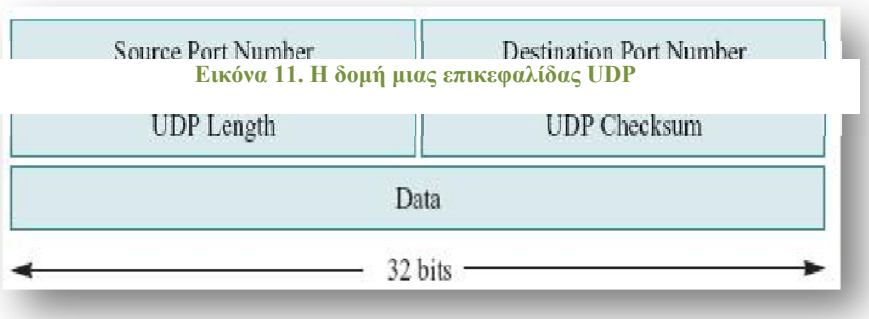
ριέχει το σχετικό αύξοντα αριθμό, σε bytes, του πρώτου byte του μηνύματος από την αρχή της επικοινωνίας. Ο αύξων αριθμός συμφωνείται από τα δύο μέρη κατά την αρχή της επικοινωνίας και είναι κάποιος (αυθαίρετος) αριθμός μήκους 32 bits. Το πεδίο *Acknowledgment Number* (μήκους 32 bits) χρησιμοποιείται για να επιβεβαιώσει τη λήψη δεδομένων. Η τιμή που περιέχει είναι η σχετική θέση του τελευταίου byte, του οποίου έγινε επιτυχής επιβεβαίωση λήψης. Το πεδίο *Header Length* (μήκους 4 bits) περιέχει το μήκος της επικεφαλίδας TCP, εκφρασμένο σε πλήθος λέξεων μήκους 32

bits. Το πεδίο *Reserved* (μήκους 6 bits) είναι δεσμευμένο για μελλοντική χρήση. Η τιμή του είναι πάντα μηδέν. Το πεδίο *Flags* (μήκους 6 bits) περιέχει τις τιμές (μήκους 1 bit η κάθε μία) των σημαφόρων που φαίνονται στον Πίνακα 3.1. Το πεδίο *Window Size* (μήκους 16 bits) περιέχει το πλήθος των bytes δεδομένων που ο αποστολέας ενός μηνύματος είναι διατεθειμένος να δεχτεί. Το πρωτόκολλο χρησιμοποιεί το πεδίο αυτό για έλεγχο ροής. Το πεδίο *TCP Checksum* (μήκους 16 bits) χρησιμοποιείται για ανίχνευση λαθών, σε αναλογία με το πεδίο *Header Checksum* της επικεφαλίδας του IPv4. Το πεδίο *Urgent Pointer* (μήκους 16 bits) υποδεικνύει το byte δεδομένων που πρέπει να υποστεί επεξεργασία πρώτο. Το πεδίο *Options* μπορεί να χρησιμοποιηθεί για τον καθορισμό διαφόρων επιλογών του πρωτοκόλλου, αλλά πολύ σπάνια χρησιμοποιείται σήμερα. Τέλος, το πεδίο *Data* περιέχει τα δεδομένα του μηνύματος TCP, μήκους το πολύ 65535 bytes.

Πρωτόκολλο UDP

Το πρωτόκολλο *User Datagram Protocol* (UDP) είναι παρόμοιο με το TCP. Κάθε μήνυμα UDP (ή τμήμα UDP) ενσωματώνεται σε ένα πακέτο IP. Επιπλέον, η έννοια των θυρών στο UDP και στο TCP είναι ίδια. Επομένως, τα πεδία *Destination Port Number* και *Source Port Number* εξυπηρετούν τους ίδιους σκοπούς που εξυπηρετούν και στο TCP. Επιπλέον, κάθε μήνυμα UDP περιέχει επίσης ένα πεδίο *UDP Length*, που δείχνει το μήκος του μηνύματος, όπως και ένα πεδίο *UDP Checksum*, που περιέχει έναν αριθμό ελέγχου για το σύνολο του μηνύματος και της επικεφαλίδας UDP. Η εικόνα 11 δείχνει τη δομή μιας επικεφαλίδας UDP.

Αντίθετα με το TCP, το UDP είναι μη αξιόπιστο πρωτόκολλο πακέτου και είναι σκόπιμα επιπόλαιο. Με το UDP, η παράδοση γίνεται στη βάση της καλύτερης προσπάθειας.



Εικόνα 11. Η δομή μιας επικεφαλίδας UDP

Δεν υπάρχει διόρθωση λαθών, αναμετάδοση ή ανίχνευση χαμένων, διπλών ή αναδιαταχθέντων πακέτων. Ακόμη και η ανίχνευση λαθών είναι προαιρετική στο UDP. Μια εφαρμογή

που χρησιμοποιεί το UDP βλέπει διακριτά μηνύματα που έχουν μήκος ακριβώς ίσο με το μέγεθος του σώματος UDP. Δεν υπάρχει στρατηγική επιβεβαίωσης ή εγγύηση αξιόπιστης παράδοσης. Βασικά, το UDP απλώς προσθέτει αριθμούς θυρών στο βασικό σχήμα παράδοσης καλύτερης προσπάθειας IP. Δεν εγγυάται την παράδοση πακέτων με τη σωστή σειρά και χωρίς επαναλήψεις ή έστω την ίδια την παράδοση. Τα μηνύματα μπορούν να χαθούν ή να φτάσουν με λάθος σειρά και είναι δουλειά της εφαρμογής που χρησιμοποιεί το UDP ως πρωτόκολλο μεταφοράς να χειριστεί τις καταστάσεις αυτές.

Από τη σκοπιά της ανάπτυξης εφαρμογών, θα ήταν άβολο κάθε εφαρμογή να επικοινωνεί απ' ευθείας με το UDP ή το TCP. Η κατασκευή TCP μηνυμάτων, όπως και οι λεπτομέρειες του ελέγχου ροής TCP, δεν χρειάζεται και δεν πρέπει να αποτελούν τμήμα ενός προγράμματος εφαρμογής. Για να διευκολυνθεί η επικοινωνία με το TCP και το UDP, έχουν αναπτυχθεί διάφορες προγραμματιστικές διεπαφές για προγραμματισμό στο επίπεδο μεταφοράς. Παραδείγματα τέτοιων διεπαφών είναιοι Berkeley sockets και η διεπαφή επιπέδου μεταφοράς (Transport Layer Interface – TLI) των συστημάτων UNIX V. Οι εφαρμογές IP που τρέχουν κάτω από Unix συνηθέστατα είναι γραμμένες για μία από τις δύο αυτές διεπαφές.

Υπάρχει μια μεγάλη ποικιλία πρωτοκόλλων εφαρμογής και υπηρεσιών που τρέχουν πάνω από το TCP και το UDP. Οι συνηθέστερες και περισσότερο χρησιμοποιούμενες εφαρμογές είναι οι εξής:

- Προσπέλαση τερματικού από απόσταση, που υλοποιείται με το πρωτόκολλο σύνδεσης από απόσταση *Telnet*.
- Μεταφορά αρχείου, που υλοποιείται με το πρωτόκολλο μεταφοράς αρχείου *File Transfer Protocol* (FTP).
- Ηλεκτρονικό ταχυδρομείο (e–mail), που υλοποιείται με το πρωτόκολλο μεταφοράς ταχυδρομείου *Simple Mail Transfer Protocol* (SMTP).

Αυτά τα πρωτόκολλα εφαρμογής υλοποιούνται πάνω από το TCP και είναι απαραίτητα για όλα τα συστήματα Internet. Το FTP έχει μια ιδιαιτερότητα, επειδή απαιτεί την εγκατάσταση δύο συνδέσεων TCP (μιας σύνδεσης ελέγχου και μιας σύνδεσης δεδομένων) μεταξύ πελάτη και εξυπηρετητή. Πέρα απ' αυτά, υπάρχουν και κάποια άλλα πρωτόκολλα εφαρμογής που υλοποιούνται πάνω από το TCP.

- Το *πρωτόκολλο μεταφοράς ειδήσεων δικτύου* Network News Transfer Protocol (NNTP), μπορεί να χρησιμοποιηθεί για την προσπέλαση και την παράδοση ειδήσεων USENET πάνω από το Internet.
- Το *πρωτόκολλο χρόνου δικτύου* Network Time Protocol (NTP) μπορεί να χρησιμοποιηθεί για το συγχρονισμό συστημάτων.
- Το *πρωτόκολλο διαχείρισης δικτύου* Simple Network Management Protocol (SNMP) μπορεί να χρησιμοποιηθεί για τη διαχείριση ετερογενών στοιχείων σε περιβάλλον Internet ή Intranet.
- Το πρωτόκολλο *X11* μπορεί να χρησιμοποιηθεί για τη διαχείριση συνόδων X–Windows μεταξύ πελατών και εξυπηρετητών X.
- Επιπλέον αυτών, υπάρχουν και κάποια πρωτόκολλα που υλοποιούνται πάνω από το UDP.
- Το *πρωτόκολλο κλήσης διαδικασίας από απόσταση* Remote Procedure Call (RPC) μπορεί να χρησιμοποιηθεί για να εκτελέσει διαδικασίες σε απόμακρα συστήματα. Το Secure RPC επεκτείνει το RPC με την υποστήριξη κρυπτογραφικής αυθεντικοποίησης. Όλες οι κλήσεις RPC αυθεντικοποιούνται χρησιμοποιώντας ένα μυστικό κλειδί, που διανέμεται χρησιμοποιώντας ανταλλαγή κλειδιών Diffie–Hellman.
- Το *σύστημα αρχείων δικτύου* Network File System (NFS) χρησιμοποιεί το RPC για να υποστηρίξει διαφανή προσπέλαση αρχείων πάνω από ένα δίκτυο. Αν υπάρχει διαθέσιμο το Secure RPC, το NFS μπορεί να το χρησιμοποιήσει.
- Παρομοίως, το *πληροφοριακό σύστημα δικτύου* Network Information System (NIS) χρησιμοποιεί το RPC για να επιτρέψει σε πολλαπλά συστήματα να μοιράζονται δεδομένα (π.χ. το αρχείο συνθηματικών) για κεντρικοποιημένη διαχείριση. Το NIS+ είναι μια ενισχυμένη μορφή του NIS, που επιτρέπει το χειρισμό μεγάλων συστημάτων και την ασφαλή ανταλλαγή κρίσιμης πληροφορίας.

Οι περισσότερες υπηρεσίες TCP/IP και τα αντίστοιχα πρωτόκολλα εφαρμογής απαιτούν κάποια μορφή αντιστοίχισης μεταξύ ονομάτων συστημάτων και των αριθμητικών τους διευθύνσεων IP. Η υπηρεσία *Domain Name Service* (DNS) επιτελεί τη λειτουργία αυτή στο Internet. Είναι η πιο ευρέως κατανεμημένη υπηρεσία σήμερα στο Internet. Ο χώρος ονομάτων DNS διαμερίζεται ιεραρχικά σε δομή δένδρου με ένα μοναδικό κόμβο ρίζας. Κάθε κόμβος ανήκει σε μια *αρχή ονοματοδοσίας*, στην οποία εναπόκειται να δημιουργήσει όσους θυγατρικούς κόμβους θέλει. Ο όρος *πεδίο*

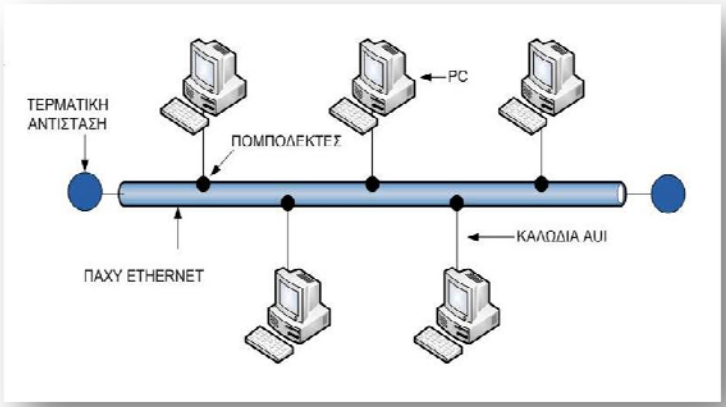
(domain) χρησιμοποιείται για να δηλώσει οποιονδήποτε κόμβο και όλους τους απογόνους του. Η αρχιτεκτονική DNS υποστηρίζεται από έναν εξυπηρετητή DNS. Ο νηθέστερα χρησιμοποιούμενος εξυπηρετητής DNS είναι ο *Berkeley Internet Name Daemon* (BIND), που αποτελεί τμήμα των περισσότερων σημερινώνσυστημάτων UNIX.

Τέλος, πρέπει να αναφέρουμε και τις διάφορες υπηρεσίες ανακάλυψης πόρων και πληροφοριών. Παραδείγματα τέτοιων υπηρεσιών είναι οι *Gopher, Wide Area Information Service* (WAIS), *World Wide Web* (WWW). Ο όρος WWW στην πραγματικότητα αναφέρεται σε ένα υπερσύνολο των FTP, Gopher, WAIS και κάποιων άλλων υπηρεσιών πληροφοριών, που υλοποιείται με το πρωτόκολλο *Hypertext Transfer Protocol* (HTTP).

1.3 Το πρωτόκολλο Ethernet

Το **Ethernet** είναι το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox, προχώρησαν στην προτυποποίησή του το 1980. Το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο **802.3** για ενσύρματα LAN.

Το αρχικό Ethernet επέτρεπε ονομαστικούς ρυθμούς μετάδοσης δεδομένων της τάξης των 3 Mbps, μέσω ενός ομοαξονικού καλωδίου στο οποίο συνδέονταν οι επιμέρους υπολογιστές του δικτύου. Τη διασύνδεση αναλάμβανε μία κάρτα δικτύου Ethernet προσαρτημένη σε κάθε κόμβο, με κάθε κάρτα να χαρακτηρίζεται από μία μοναδική, εργοστασιακή 48-bit διεύθυνση MAC. Σήμερα έχουν εμφανιστεί νεότερες εκδόσεις του Ethernet με επιτρεπτούς ρυθμούς μετάδοσης δεδομένων μέχρι 10Gbps.



Εικόνα 12. Ethernet Δίκτυο

Οι ραφές που ορίζει το Ethernet αφορούν το φυσικό επίπεδο και το υποεπίπεδο MAC του μοντέλου αναφοράς OSI. Στη μεγάλη πλειονότητα των περιπτώσεων μαζί με το Ethernet χρησιμοποιείται, στο υποεπίπεδο LLC, το πρωτόκολλο IEEE 802.2. Για τον έλεγχο πρόσβασης στο κοινό μέσο το Ethernet αξιοποιεί τον αλγόριθμο CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Παχύ Ethernet (Thicknet, 10Base5)

Ο τρόπος καλωδίωσης του αρχικού Ethernet λέγεται άτυπα Ethernet με παχύ καλώδιο (Thick wire Ethernet ή Thicknet) επειδή το μέσο επικοινωνίας είναι ένα παχύ ομοαξονικό καλώδιο. Επιστημονικά αυτός ο τρόπος λέγεται 10Base5. Η κάρτα διασύνδεσης δικτύου (NIC- Network Interface Card) περιέχει κυκλώματα που χειρίζονται τις ψηφιακές πλευρές της επικοινωνίας, όπου είναι η ανίχνευση σφαλμάτων και η αναγνώριση διευθύνσεων. Η κάρτα διασύνδεσης δικτύου που χρησιμοποιείται σε αυτό τον τύπο δικτύου (Thicknet) δεν περιέχει αναλογικό υλικό και δεν χειρίζεται τα αναλογικά σήματα. Αυτήν την δουλεία την αναλαμβάνει μία εξωτερική συσκευή που ονομάζεται πομποδέκτης (Transceiver). Ο πομποδέκτης συνδέεται απευθείας με το καλώδιο του Ethernet και με ένα άλλο τύπο καλωδίου με την κάρτα διασύνδεσης δικτύου.

Το καλώδιο που συνδέει την κάρτα διασύνδεσης δικτύου με τον πομποδέκτη λέγεται καλώδιο AUI (Attachment Unit Interface → Διασύνδεση μονάδας προσάρτησης), και οι συζευκτήρες στην κάρτα διασύνδεσης δικτύου και πομποδέκτη λέγονται συζευκτήρες AUI. Το καλώδιο AUI περιέχει πολλά σύρματα, τα βασικά είναι μόνο δύο. Τα υπόλοιπα χρησιμοποιούνται για τον έλεγχο και την τροφοδοσία του πομποδέκτη.

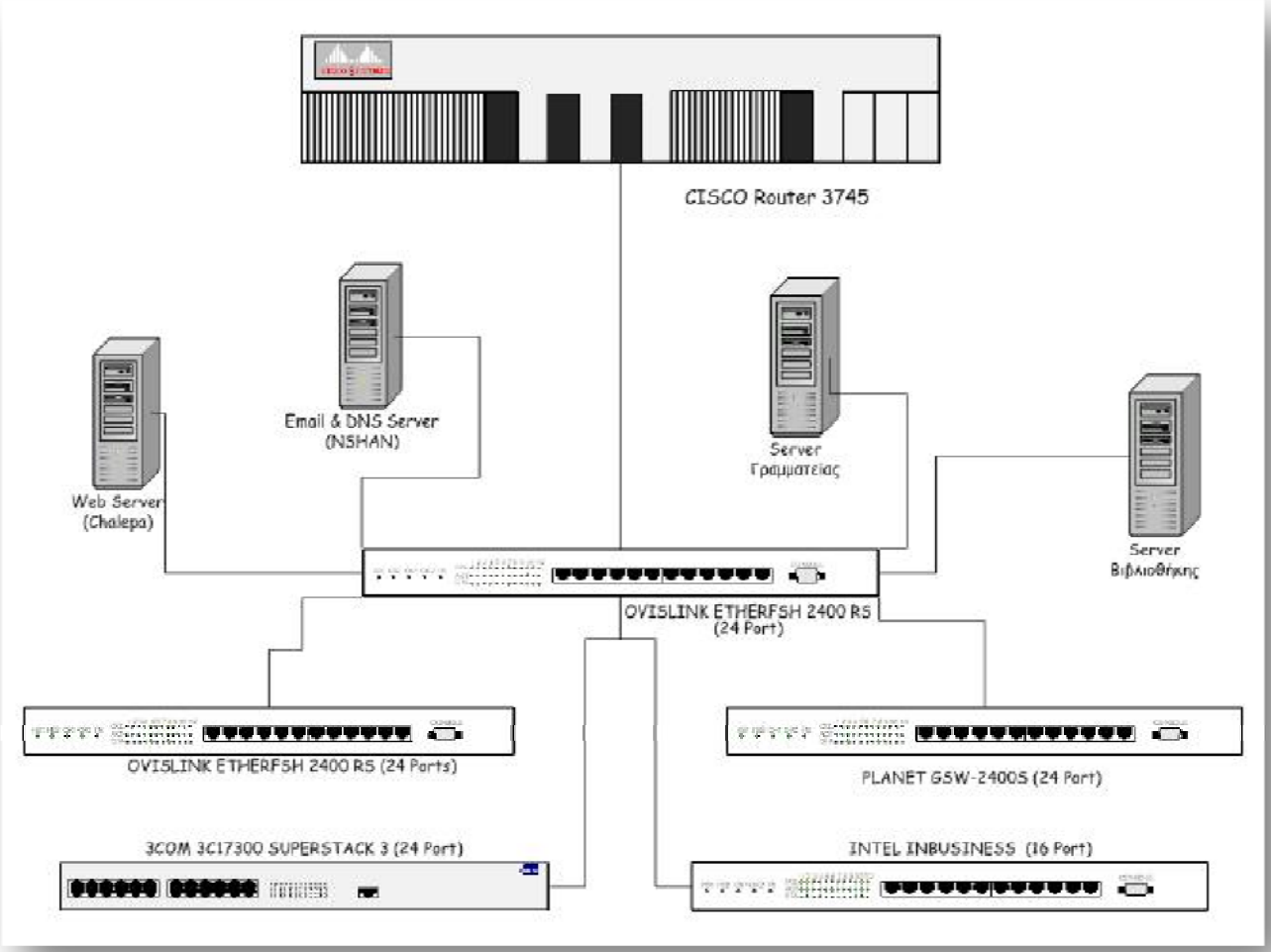
Υπάρχουν περιπτώσεις όπου η καλωδίωση που χρησιμοποιείται στο παχύ Ethernet δεν είναι βολική. Μία τέτοια περίπτωση είναι να υπάρχουν πολλοί υπολο-

γιστές σε μία αίθουσα ενός πανεπιστημίου. Αν το καλώδιο του Ethernet είναι έξω από την αίθουσα θα πρέπει να εγκαταστήσουμε στο διάδρομο όλα τα καλώδια AUI που θα ενώνουν τους υπολογιστές με τους πομποδέκτες, επίσης το πρότυπο του Ethernet καθορίζει μία ελάχιστη απόσταση μεταξύ δύο πομποδεκτών. Για να αντιμετωπιστεί το πρόβλημα των πολλών υπολογιστών σε μία αίθουσα οι μηχανικοί έχουν επινοήσει κάποιες συσκευές που ονομάζονται πολυπλέκτες συνδέσεων (Connections multiplexors). Ένας πολυπλέκτης συνδέσεων επιτρέπει να συνδέονται πολλοί υπολογιστές στον ίδιο πομποδέκτη.

ΚΕΦΑΛΑΙΟ 2^{0}

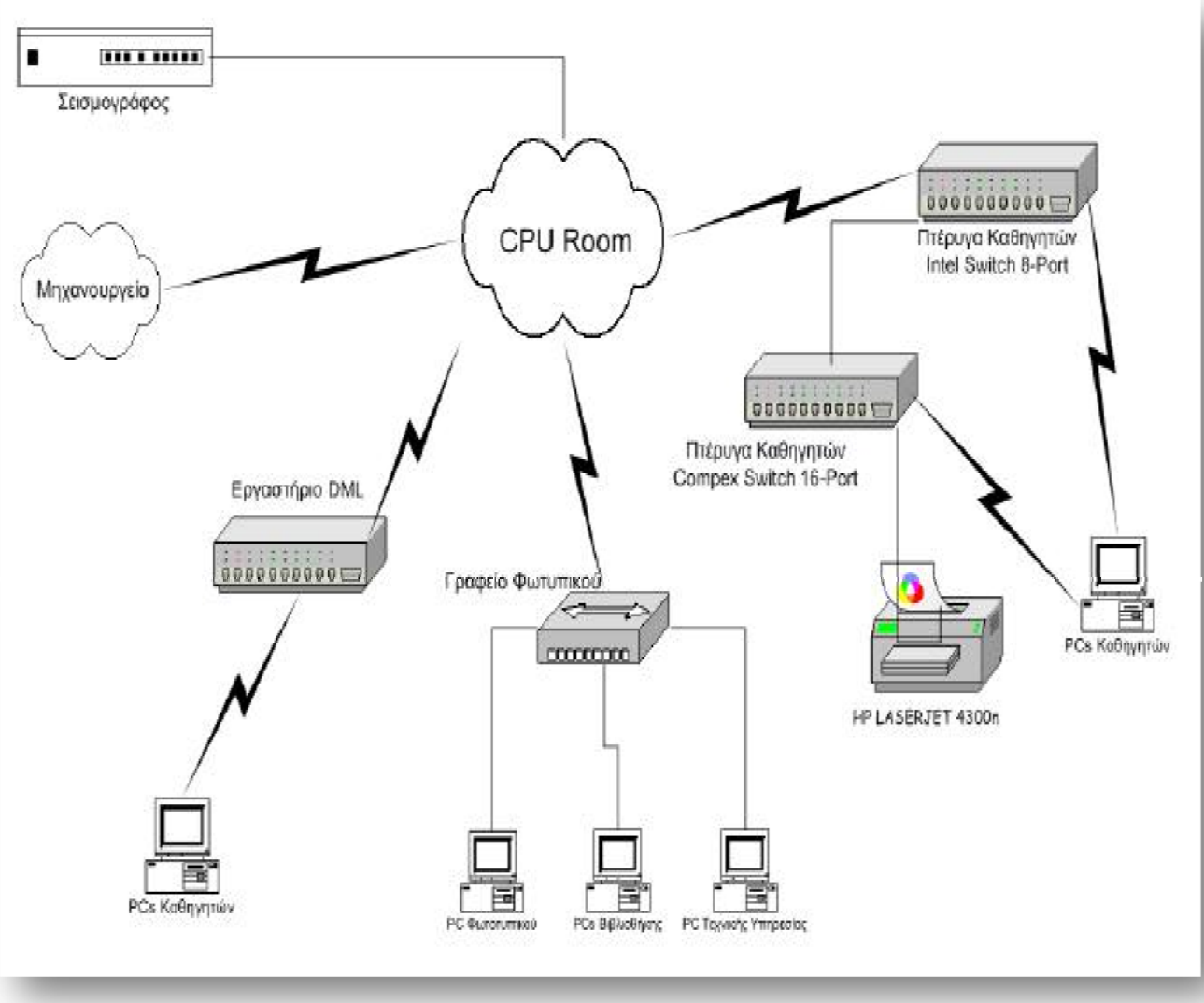
2.1 Τεχνικός εξοπλισμός κτηρίου

COMPUTER ROOM



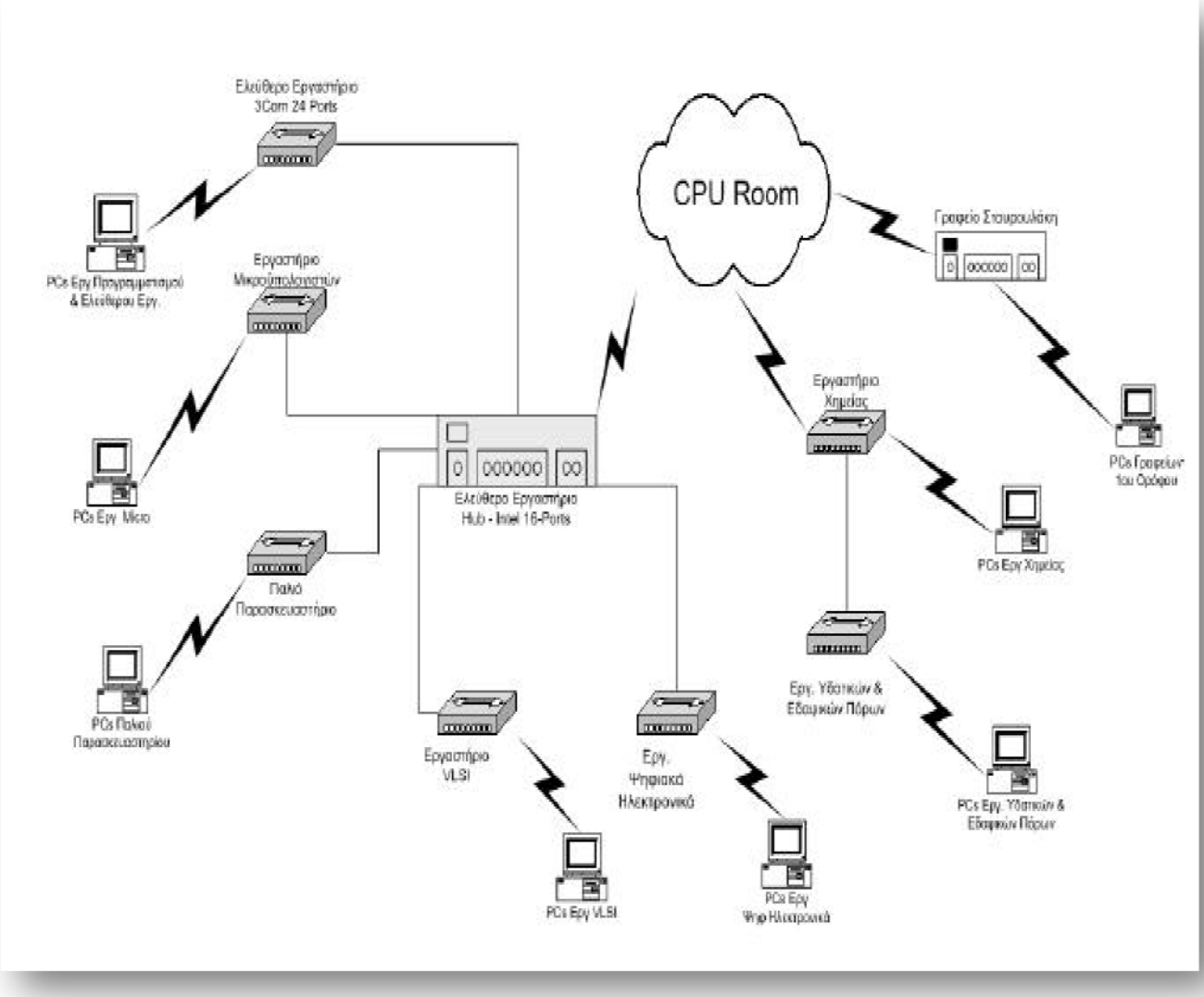
Εικόνα 13. Τοπολογικό σχέδιο του Computer Room

Ισόγειο - Υπόγειο



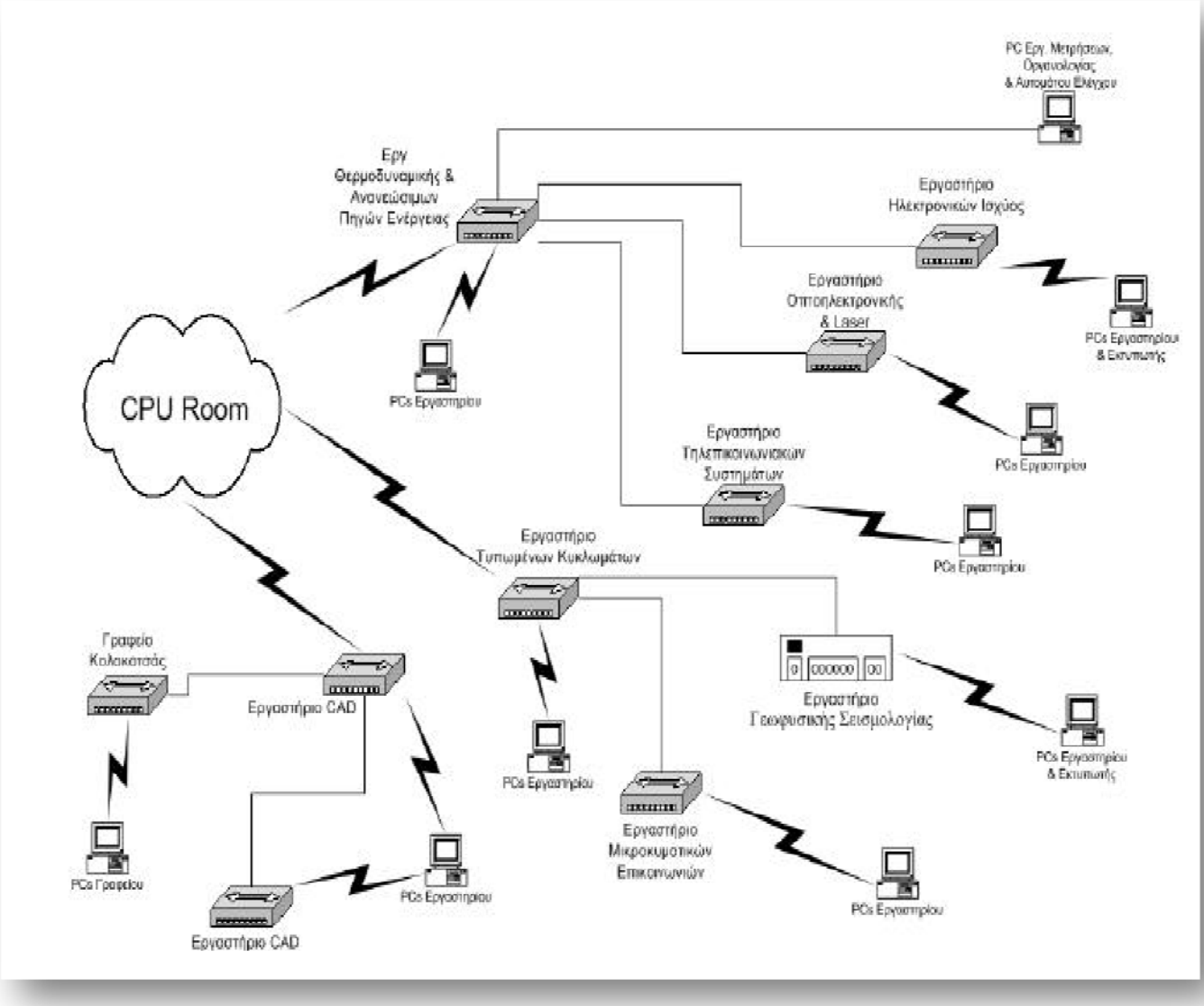
Εικόνα 14. Τοπολογικό σχέδιο Υπογείου - Ισογείου

1ος Όροφος



Εικόνα 15. Τοπολογικό σχέδιο 1ου Ορόφου

2ος Όροφος



Εικόνα 16. Τοπολογικό σχέδιο 2ου ορόφου

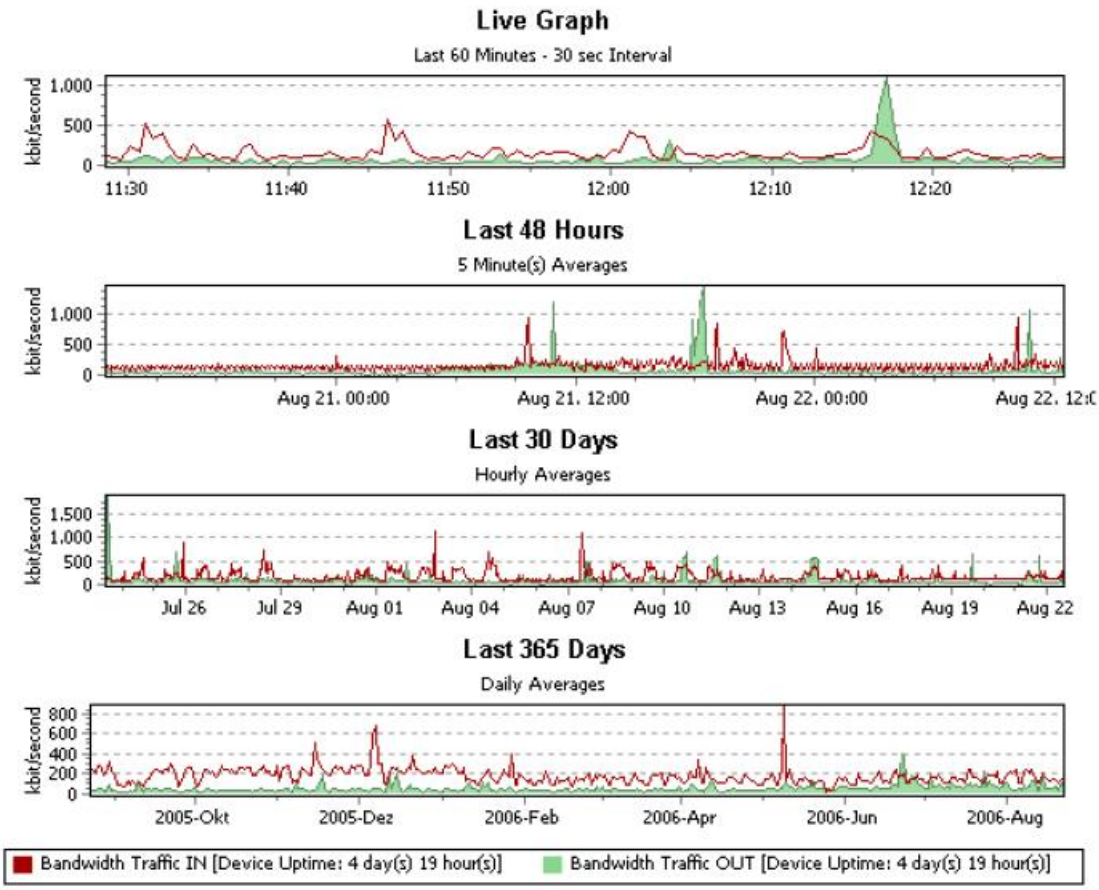
2.2 PRTG Traffic Grapher v.6.0

PRTG (Paessler Router Traffic Grapher) is an easy to use software that monitors bandwidth usage and many other network parameters via SNMP, Packet Sniffing, or Cisco NetFlow. It allows you to quickly and easily set up and run a monitoring station for networks. With just a few mouse clicks you can log the amount of data flowing through routers and leased lines, monitor CPU utilization, analyze the traffic by type, or check disk space usage.

The most common usage is monitoring the bandwidth usage of leased lines, routers, and firewalls via SNMP, packet sniffing, or NetFlow. But you can also monitor many other aspects of servers, managed switches, printers, and other network components, as long as they are SNMP enabled.

PRTG Traffic Grapher runs on a Windows machine in your network for 24 hours every day and constantly records the network usage parameters. The recorded data is stored in an internal database for later reference.

Here are two sample graphs showing the usage of a 2 MBit/s leased line over various time periods:



Εικόνα 17. Μετρήσεις Bandwidth

The recorded monitoring statistics can be viewed in the Windows GUI of PRTG Traffic Grapher. Also, all aspects of the configuration of the sensors is done using the Windows GUI.

For remote access to the monitoring results PRTG Traffic Grapher comes with a built in web server for easy access to graphs and tables using a web browser.

For data acquisition the three most common methods for bandwidth monitoring are supported:

- Using SNMP (Simple Network Management Protocol) to access traffic counters or other readings from SNMP enabled devices (most common)
- Looking at incoming/outgoing network packets that pass through a network card of a computer (so called “packet sniffing”)
- Analyzing Cisco NetFlow packets send by Cisco routers

Included with the installer is the tool “Paessler SNMP Helper (Freeware Edition)” which drastically eases accessing various system readings on Windows 2000/XP/2003 systems via SNMP which usually is very complicated. Optional Pro

Editions of SNMP Helper are also available for Exchange, SQL, ISA, and Biztalk Server, see www.paessler.com/snmphelper.

PRTG Traffic Grapher is available in both a Freeware edition (limited to monitoring up to three network devices and suitable for home users and SOHOs) and several commercial editions offering monitoring for multiple network devices and advanced features needed by companies.

ΚΕΦΑΛΑΙΟ 3ο

3.1 Εισαγωγή στις μετρήσεις

Για την πραγματοποίηση μιας μελέτης οι μετρήσεις είναι ένας σημαντικός παράγοντας που βοηθάει τόσο στην κατανόηση του θέματος όσο και στην αποτελεσματικότητα της. Μια μέτρηση είναι η εικόνα και πιθανώς η εύρεση ενός προβλήματος. Ένα σύνολο όμως μετρήσεων με σωστά προκαθορισμένο πλήθος και για προκαθορισμένη χρονική διάρκεια αποτελεί ίσως τη λύση αυτού του προβλήματος.

Η καταγραφή της κίνησης του δικτύου μπορεί να πραγματοποιηθεί και να χαρακτηριστεί λαμβάνοντας πλήθος μετρήσεων με συγκεκριμένο λογισμικό. Με τον όρο κίνηση εννοούμε το πλήθος των πληροφοριών που εισέρχονται και εξέρχονται σ' ένα δίκτυο. Για παράδειγμα σ' ένα δίκτυο 200 υπολογιστών η επικοινωνία τόσο μεταξύ τους όσο και του κάθε υπολογιστή ξεχωριστά με τον κυβερνοχώρο γίνεται με την δρομολόγηση κάποιων πακέτων. Το πλήθος, η ταχύτητα και η προτεραιότητα αυτών των πακέτων αποτελούν την κίνηση (traffic) του δικτύου. Για την λήψη όλων αυτών των πληροφοριών πρέπει να έχουμε την συνεργασία

του κεντρικού υπολογιστή ο οποίος καλείτε στο δίκτυο μας ως πύλη και δρομολογεί μέσω του router τον όγκο των πακέτων στα επί μέρους switches (μεταγωγείς) για να φτάσουν στη αντίστοιχη θέση εργασίας.

Το πλήθος λοιπόν αυτών των μετρήσεων διαχωρίζονται στα παρακάτω είδη :

- Εισερχόμενη και εξερχόμενη κίνηση ανά interface δρομολογητή ή μεταγωγέα σε ρυθμό bits και πακέτων ανά δευτερόλεπτο.
- Εισερχόμενη και εξερχόμενη κίνηση ανά interface δρομολογητή όλων των κλάσεων
- QoS που ορίζονται ανά interface, με δυνατότητα καταγραφής και της κίνησης που υπερβαίνει τα προκαθορισμένα όρια.
- Εισερχόμενη και εξερχόμενη κίνηση ανά interface δρομολογητή της κίνησης multicast σε ρυθμό bits/sec.
- Απεικόνιση του συνολικού δένδρου προώθησης multicast και ανά multicast group (multicast weathermap),

Τα παραπάνω στοιχεία αλλά με περισσότερη ανάλυση που να φανερώνει τα ποσοστά ανά έκδοση IP και πρωτόκολλο (TCP,UDP κλπ.), πόρτα πρωτοκόλλου κλπ.

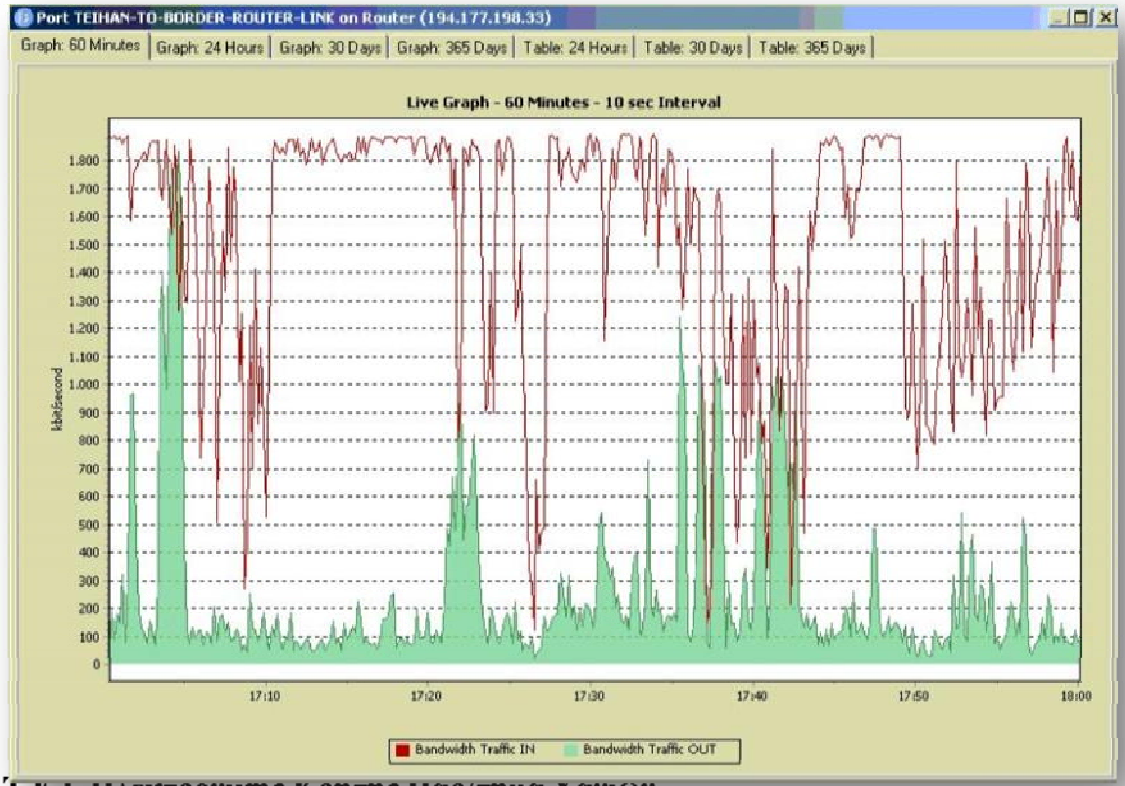
3.2 Μετρήσεις Bandwidth (Γραφική απεικόνιση)

Υπάρχει μία πολύ ακριβής και τεχνική ερμηνεία του όρου bandwidth, αλλά σε μία απλή μετάφραση θα μπορούσαμε να ορίσουμε τον όρο αυτό ως την ταχύτητα ροής των πληροφοριών από το ένα μέρος της σύνδεσης στο άλλο. Η σύνδεση μεταξύ των δύο σημείων στα οποία μεταφέρονται οι πληροφορίες ονομάζεται δίκτυο. Μία συνήθης αναλογία είναι αυτή των καναλιών επικοινωνίας με τις σωλήνες ύδρευσης και των πληροφοριών με το νερό. Ένα κανάλι επικοινωνίας, όπως και ο σωλήνας ύδρευσης έχει ένα εύρος και επιτρέπει ορισμένο ποσό πληροφοριών – νερού να περάσει από αυτό. Στις επικοινωνίες, το bandwidth είναι το ποσό των πληροφοριών οι οποίες ρέουν μέσα από ένα κανάλι. Το bandwidth μετριέται συνήθως σε bits/sec. Ο αριθμός

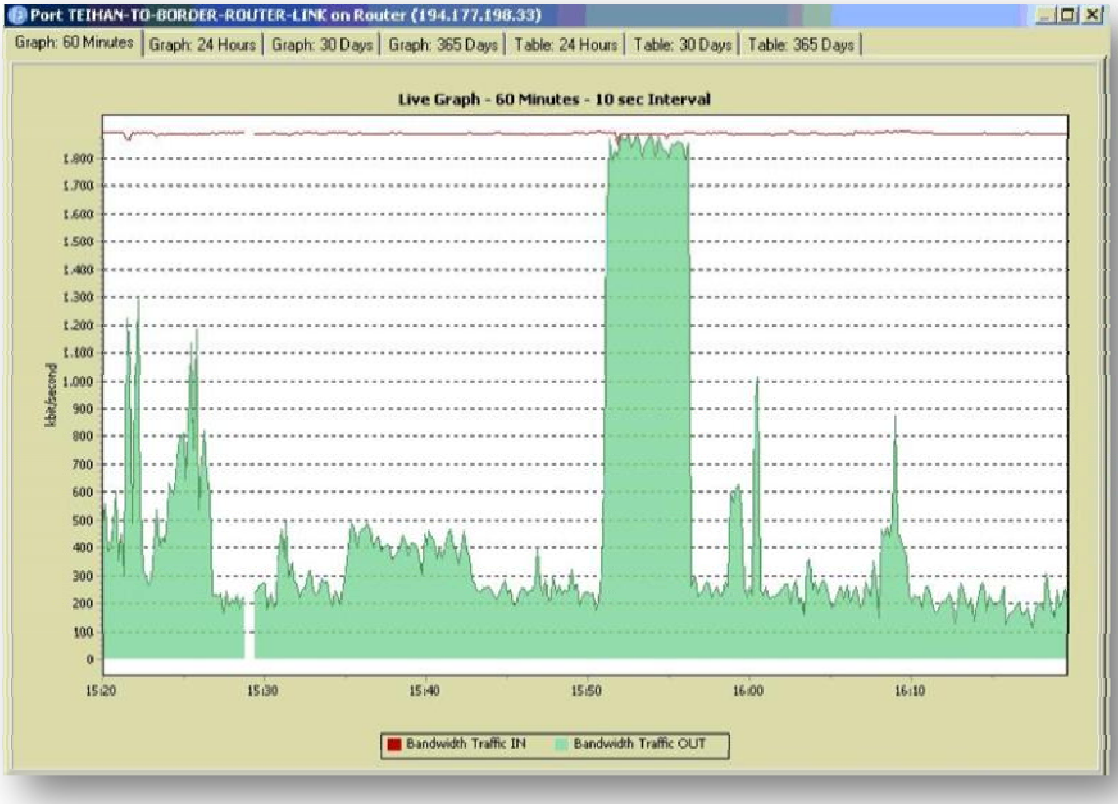
αυτός είναι μία απλή αναλογία που αναφορικά με την παραπάνω αντιστοιχία είναι τα κυβικά μέτρα νερού που διέρχονται τον σωλήνα σε κάθε δευτερόλεπτο. Γνωρίζοντας επίσης ότι η συνηθέστερη αναλογία της εποχής μας είναι η ταχύτητα μπορούμε να πούμε ότι τα bits/sec είναι όπως τα km/h και το bandwidth είναι το όριο ταχύτητας με μόνη διαφορά ότι δεν μπορούμε να το ξεπεράσουμε. Έτσι αν θέλουμε να μεταφέρουμε ένα αρχείο του υπολογιστή με μέγεθος 1Mbyte διαμέσου μίας τηλεφωνικής γραμμής με bandwidth περίπου 8kbits/sec τότε θα χρειαστούμε περίπου 1.000 sec ή 17 λεπτά.

Η πραγματοποίηση των μετρήσεων έγινε συγκεκριμένο χρονικό διάστημα και από συγκεκριμένο υπολογιστή ο οποίος ρυθμίστηκε ώστε να έχει access στην καταγραφή πληροφοριών του δικτύου από συγκεκριμένη πόρτα πάνω στο switch. Η διαδικασία αυτή έγινε στο computer room της σχολής προκειμένου να τηρηθούν όλοι οι κανόνες ασφαλείας των μετρήσεων για να μην έχουμε παραποίηση στα αποτελέσματα, καθώς επίσης και να διασφαλιστεί η καταγραφή προσωπικών δεδομένων που μπορεί να έγινε με τη χρήση του PRTG.

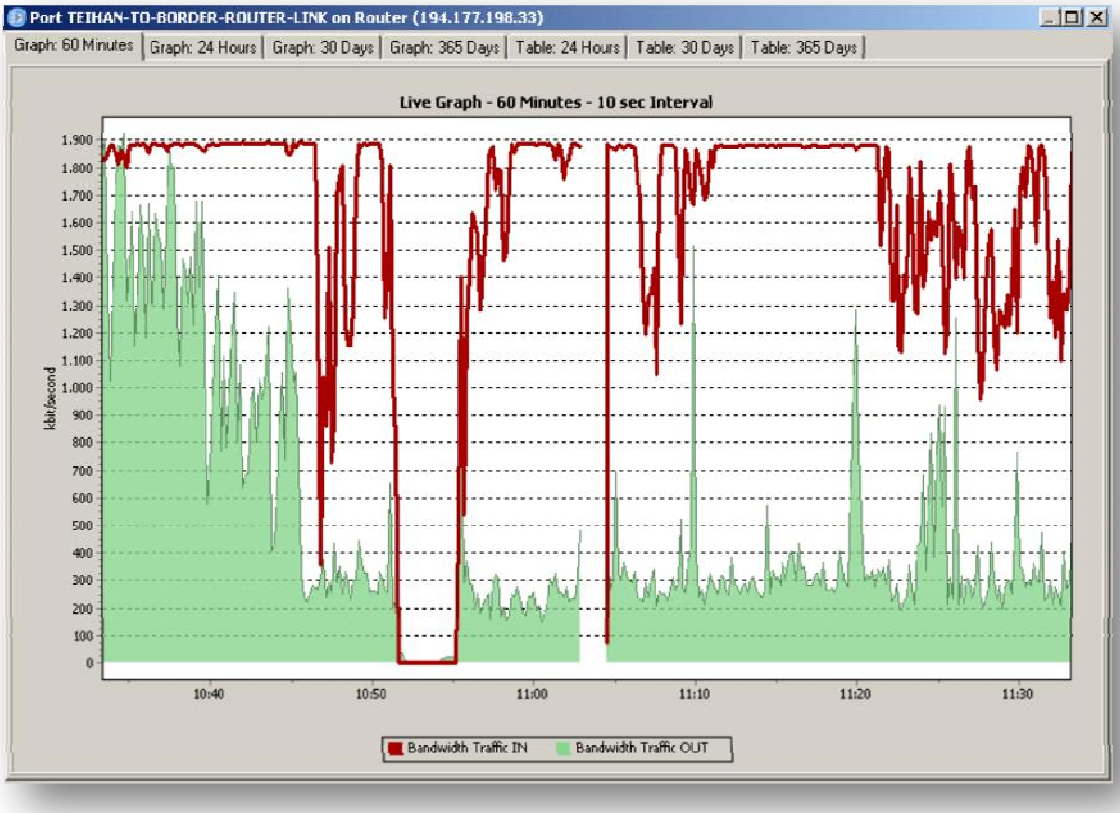
3.2.1 Ωριαίες μετρήσεις



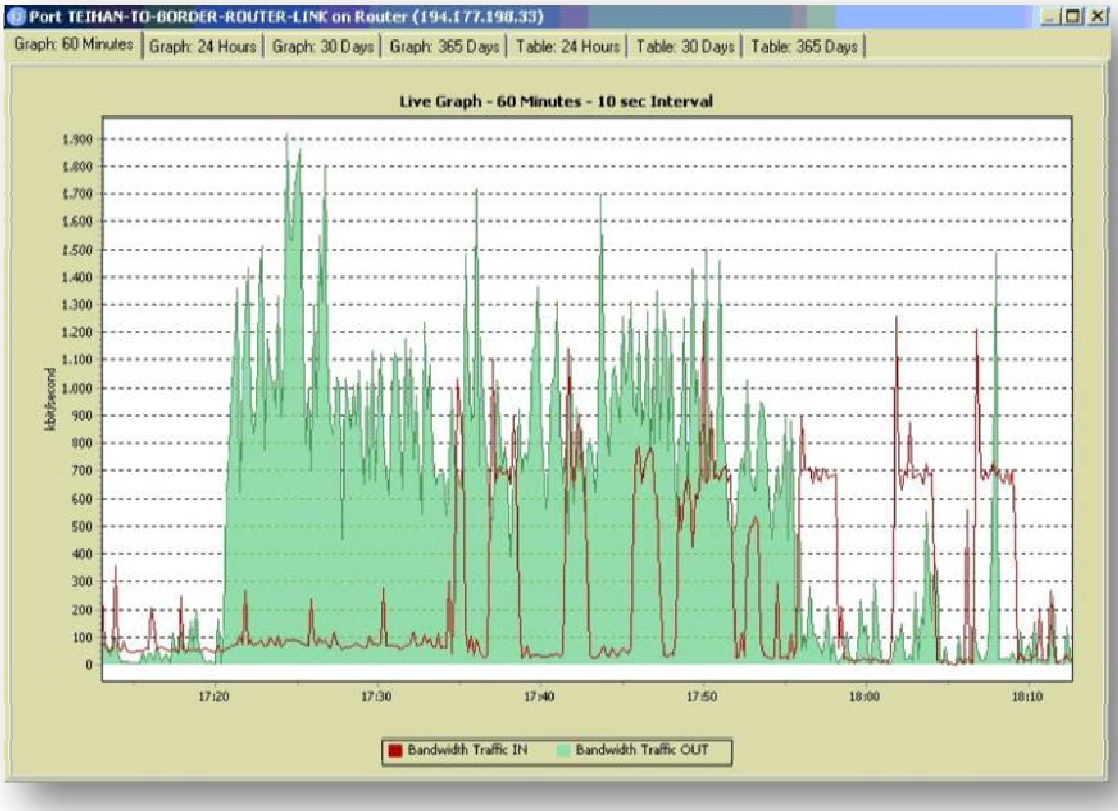
Εικόνα 18



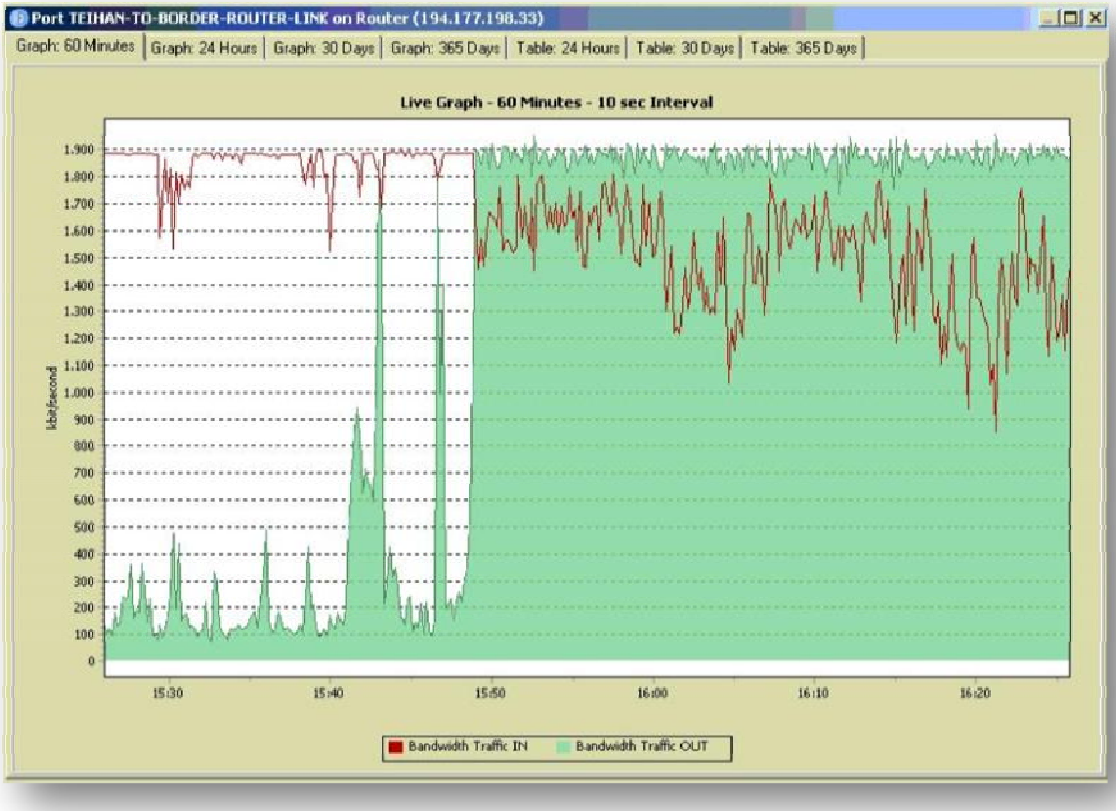
Εικόνα 19



Εικόνα 20

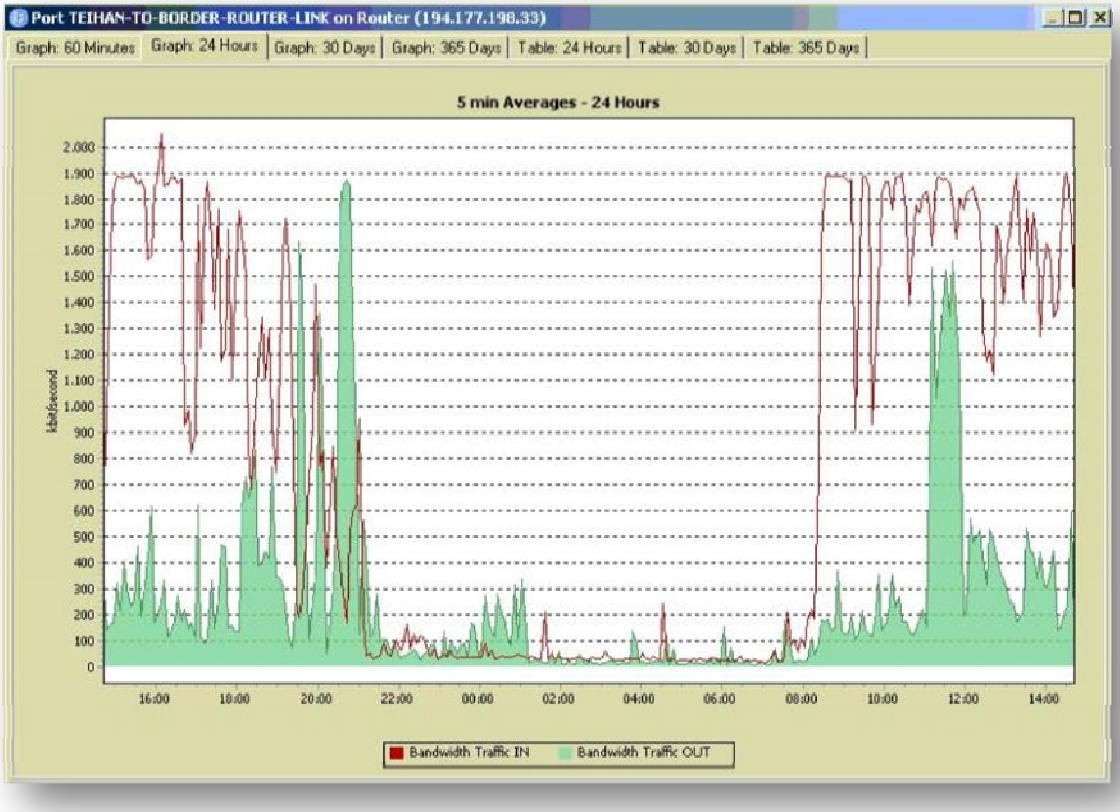


Εικόνα 21

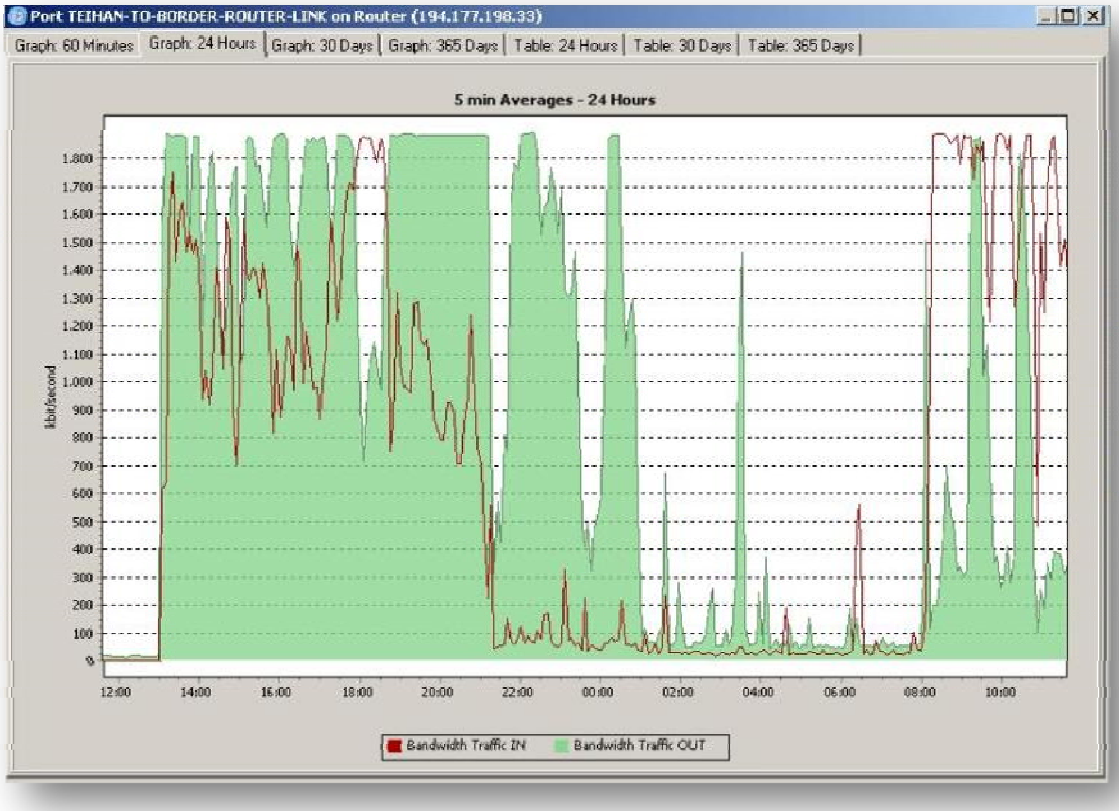


Εικόνα 22

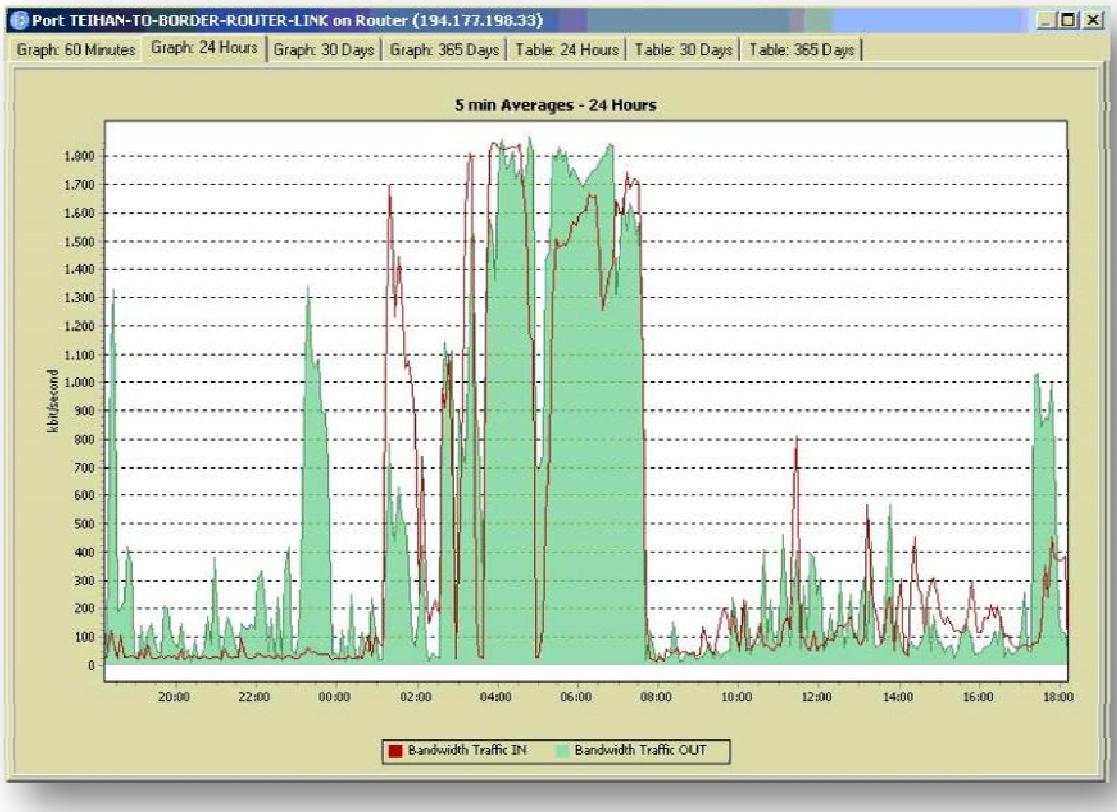
3.2.2 Ημερήσιες μετρήσεις



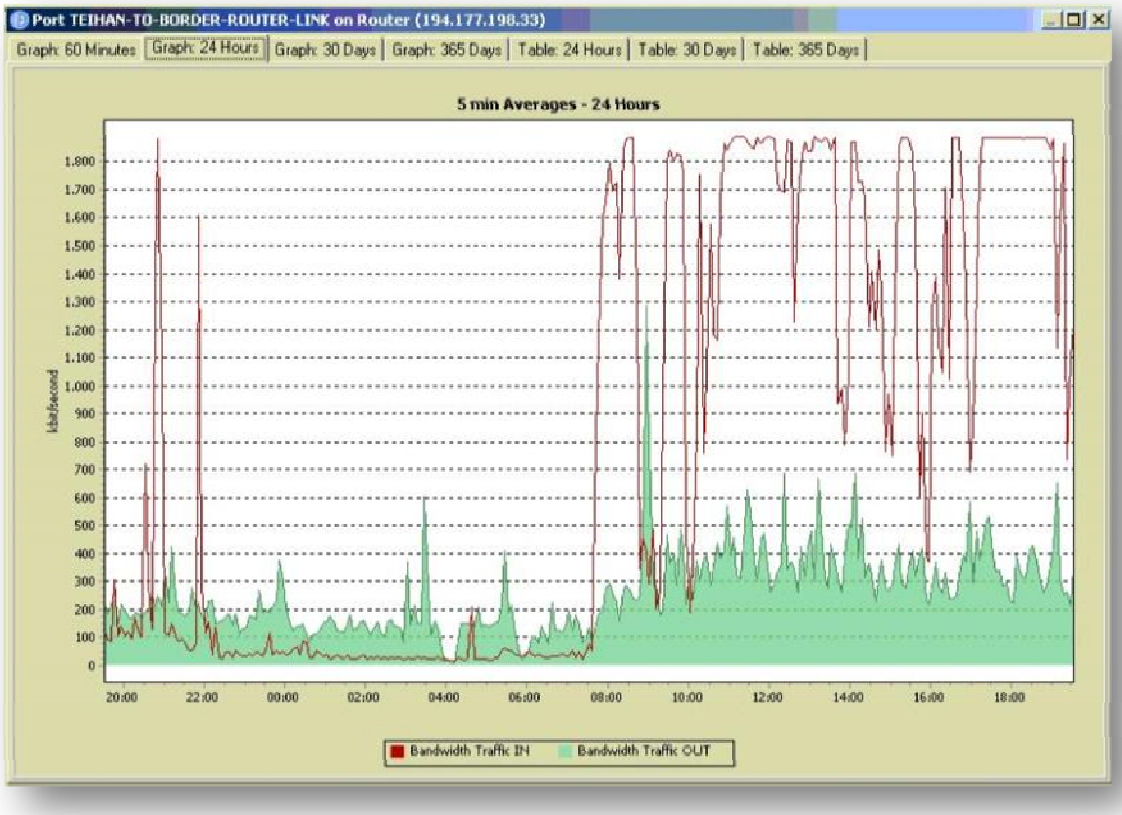
Εικόνα 23



Εικόνα 24

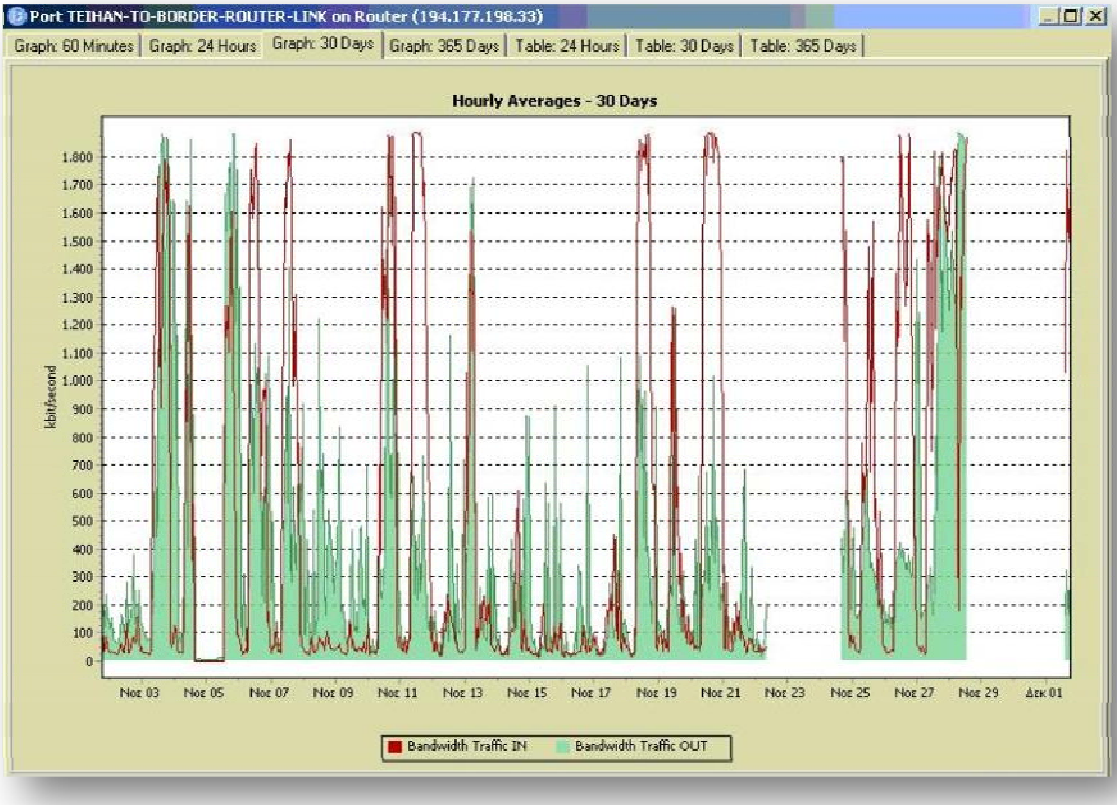


Εικόνα 25

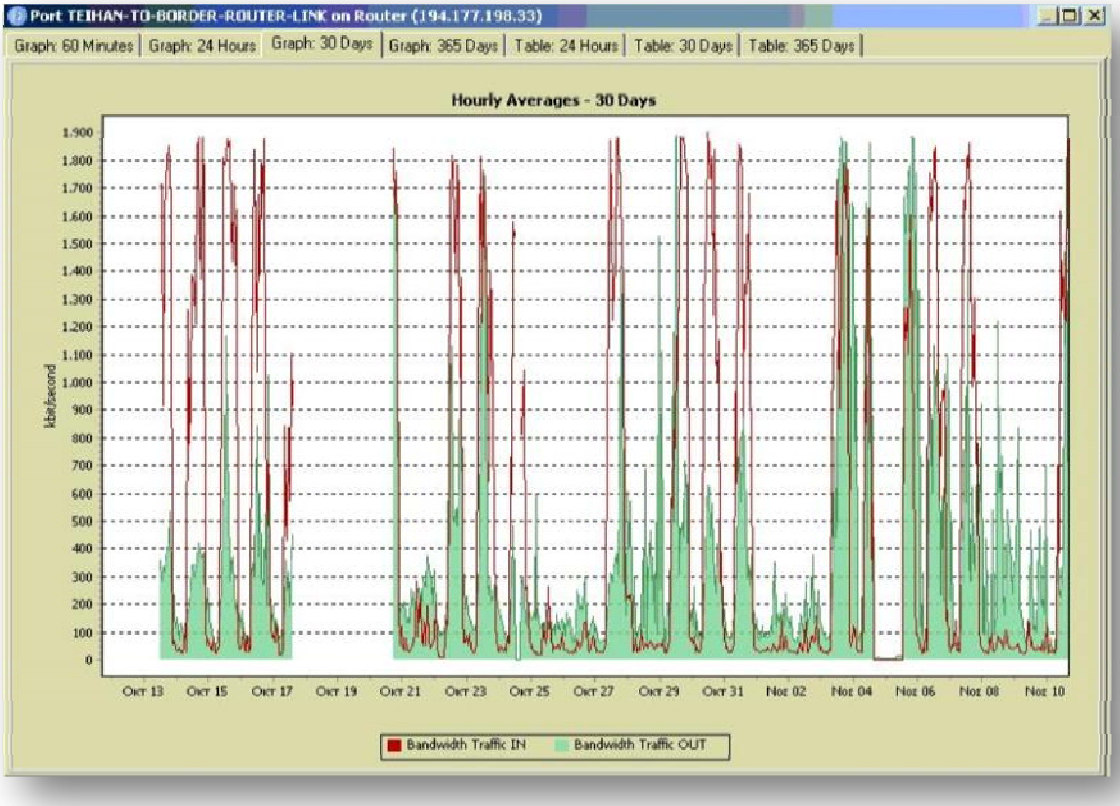


Εικόνα 26

3.2.3 Μηνιαίες μετρήσεις

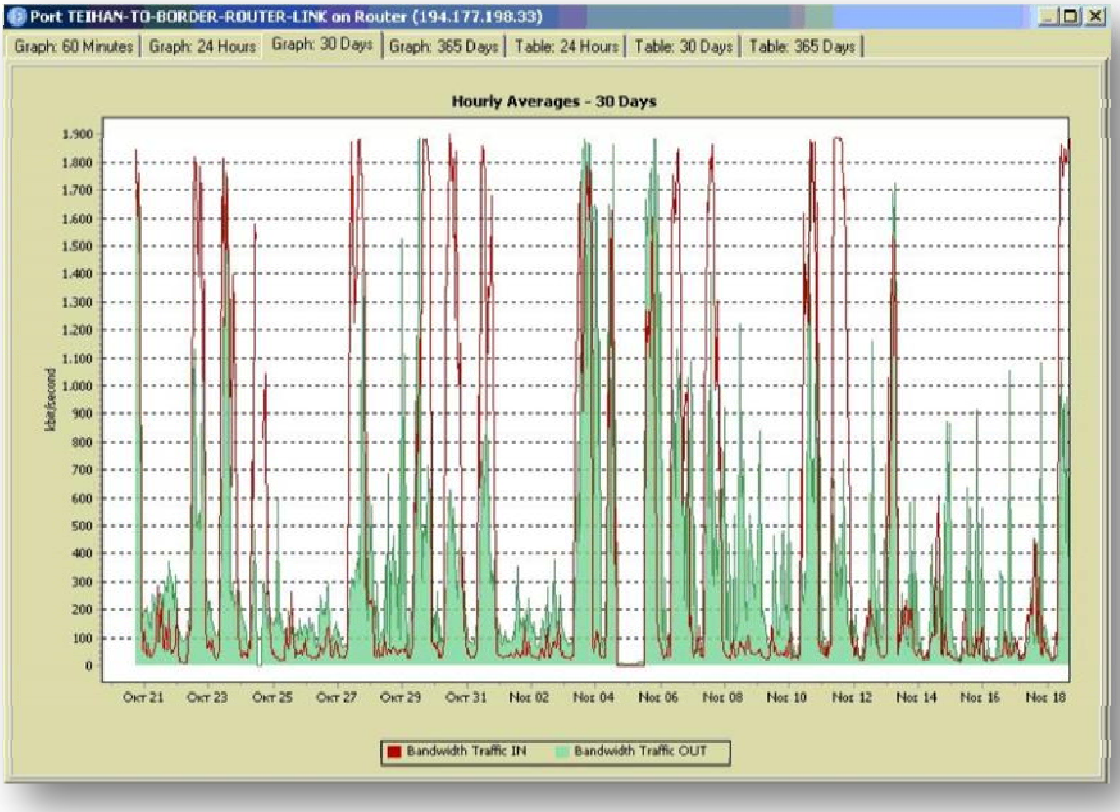


Εικόνα 27



Εικόνα 28

Εικόνα 29


Port TEIHAN-TO-BORDER-ROUTER-LINK on Router (194.177.198.33)
Graph: 60 Minutes
Graph: 24 Hours
Graph: 30 Days
Graph: 365 Days
Table: 24 Hours
Table: 30 Days
Table: 365 Days
Hourly Averages - 30 Days
kbps/second
Bandwidth Traffic IN
Bandwidth Traffic OUT

Εικόνα 30

3.3 Ανάλυση των μετρήσεων

Η καταγραφή της κίνησης του δικτύου πραγματοποιήθηκε την περίοδο 30/10/2008 έως 5/12/2008 και από 22/04/2009 έως 22/05/2009 . Μέσα από ένα μεγάλο κομμάτι δεδομένων που αφορούν το Bandwidth του δικτύου προβάλλονται γραφικά οι μετρήσεις που παρουσιάζουν το μεγαλύτερο ενδιαφέρον. Στα παραπάνω γραφήματα εμφανίζονται δυο μετρήσεις, με κόκκινο διαγράφεται το Bandwidth traffic In δηλαδή το Download που πραγματοποιείτε από τους χρήστες του δικτύου, ενώ με πράσινο είναι η περιοχή του Bandwidth traffic Out δηλαδή το Upload που γίνεται στο δίκτυο. Πρόκειται για ένα γράφημα της ταχύτητας του δικτύου σε kbit/sec συναρτήσει του χρόνου. Με την δυνατότητα των ωριαίων ,ημερήσιων και μηνιαίων μετρήσεων που μπορεί να μας δώσει το PRTG Grapher v.6.0 έχουμε μια αναλυτικότερη παρουσίαση της κατάστασης που επικρατεί στο δίκτυο , καθώς βλέπουμε συγκεκριμένες ώρες και μέρες που η κίνηση χρησιμοποιεί τη μέγιστη απόδοση του δικτύου όπου και παρουσιάζεται το πρόβλημα υπερφόρτωσης, έχοντας ως αποτέλεσμα τις γνωστές σε όλους μας καθυστερήσεις στο άνοιγμα κάποιας ιστοσελίδας , την καθυστέρηση κάποιου streaming video, την αδυναμία αποστολής κάποιου e-mail κ.α.

Από τις μετρήσεις που παρουσιάζονται παραπάνω είναι προφανές ότι η χρήση του bandwidth σε ώρες λειτουργίας της σχολής φτάνει στο 100%. Αυτό υπο συνθήκες οικιακής χρήσης του internet δεν αποτελεί πρόβλημα, στη προκειμένη το bandwidth του δικτύου μπορεί να φτάσει στο μέγιστο από έναν και μόνο υπολογιστή. Όπως έδειξαν οι πίνακες των μετρήσεων μόνο μια IP διεύθυνση κάθε φορά χρησιμοποιεί το μέγεθος που χρειάζεται και οι υπόλοιπες απλά ότι απομένει. Η αντιμετώπιση αυτού του προβλήματος βρίσκεται σε δικτυακές εφαρμογές που ορίζουν σε κάθε IP το μέγιστο bandwidth που μπορεί να καταναλωθεί. Σε αυτό το σημείο αξίζει να σημειωθεί ότι στη σχολή κάτι τέτοιο είναι αδύνατο με την υπάρχουσα γραμμή των 2Mbit/sec

Δυστυχώς στην Ελλάδα το πρόβλημα αυτό είναι σύνηθες, δεδομένου ότι στο κλάδο των τηλεπικοινωνιών η χώρα έχει μείνει αρκετά πίσω με αποτέλεσμα η ζήτηση των πληροφοριών που απαιτούνται από έναν χρήστη του διαδικτύου να είναι δυσανάλογη των ταχυτήτων που προσφέρονται από τις εταιρίες παροχής internet.

ΚΕΦΑΛΑΙΟ 4ο

4.1 Packet Sniffer

Το Packet sniffer επίσης αποκαλούμενο *network monitor* ή *network analyzer*, είναι λογισμικό με δυνατότητα παρακολούθησης των πακέτων ενός δικτύου. Όταν γίνει αντιληπτό κάποιο πακέτο το οποίο ικανοποιεί συγκεκριμένα κριτήρια, καταγράφεται σε ένα αρχείο.

Για πολύ καιρό οι μηχανικοί δικτύων, διαχειριστές συστημάτων και επαγγελματίες στον τομέα της ασφάλειας, αλλά και crackers, κάνουν χρήση ανάλογων εργαλείων. Χρησιμοποιείται νόμιμα από τους πρώτους για καταγραφή και διορθώσεις στην κίνηση (traffic) του δικτύου.

4.1.0.1 Τρόπος λειτουργίας

Οι περισσότεροι προσωπικοί υπολογιστές συνδέονται σε ένα LAN (Local Area Network - Τοπικό Δίκτυο), που σημαίνει ότι μοιράζονται μία σύνδεση με άλλους υπολογιστές. Αν το δίκτυο δεν χρησιμοποιεί switch (μεταγωγείς) - μεταγωγέας είναι μια συσκευή που φιλτράρει και ξαναστέλνει τα πακέτα ανάμεσα στους τομείς ενός LAN - η κίνηση που προορίζεται για έναν τομέα μεταδίδεται σε κάθε μηχάνημα του δικτύου. Επακόλουθα, κάθε υπολογιστής στην πραγματικότητα βλέπει τα δεδομένα που προέρχονται από ή προορίζονται για τους γειτονικούς υπολογιστές, αλλά τα αγνοεί.

Ένα πακέτο sniffer μπορεί να χρησιμοποιηθεί και στο Διαδίκτυο για την συλλογή των δεδομένων που ταξιδεύουν μεταξύ των υπολογιστών. Τα πακέτα του Internet έχουν συχνά πολύ μεγάλες αποστάσεις για να ταξιδεύουν, να διέρχεται από πολλές δρομολογητών που ενεργούν ως ενδιάμεσοι ταχυδρομικά γραφεία.

Ένα πακέτο sniffer μπορεί να εγκατασταθεί σε οποιοδήποτε σημείο στην πορεία. Θα μπορούσε επίσης να εγκαταστήσει λαθραία σε ένα διακομιστή που λειτουργεί ως πύλη ή συλλέγει προσωπικές πληροφορίες ζωτικής σημασίας. Το sniffer αναγκάζει τον υπολογιστή, συγκεκριμένα την Network Interface Card (NIC), να αρχίσει

να προσέχει και αυτά τα πακέτα, τα οποία προορίζονται για άλλους υπολογιστές. Για να το καταφέρει αυτό θέτει τη NIC σε ειδική λειτουργία, γνωστή ως promiscuous mode. Όταν η NIC βρίσκεται σε αυτή τη λειτουργία, μια κατάσταση που συνήθως απαιτεί δικαιώματα ανώτερου χρήστη (root), ένα μηχάνημα μπορεί να βλέπει όλα τα δεδομένα που μεταδίδονται στον τομέα του.

Υπάρχουν πολλές δυνατότητες, που καθορίζουν την τύχη των πακέτων:

- Τα πακέτα μετριούνται. Με αυτό τον τρόπο, προσθέτοντας στη συνέχεια το συνολικό μέγεθός τους για μία ορισμένη χρονική περιόδο (συμπεριλαμβάνοντας τις επικεφαλίδες των πακέτων), εξάγεται μια καλή ένδειξη για το πόσο φορτωμένο είναι το δίκτυο. Το πρόγραμμα μπορεί να παρέχει γραφικές απεικονίσεις της σχετικής κίνησης του δικτύου.
- Τα πακέτα μπορούν να εξετασθούν λεπτομερώς. Είναι δυνατόν να γίνει σύλληψη συγκεκριμένων πακέτων, ώστε να διαγνωσθεί και να αντιμετωπιστεί ένα πρόβλημα.

4.1.0.2 Προστασία από sniffers & Εργαλεία Anti-Sniffing

Συνήθως, ένα packet sniffer έχει passive (παθητική) λειτουργία. Απλώς συλλαμβάνει πακέτα που ταξιδεύουν μέσω της network interface card (NIC) την οποία ελέγχει. Για αυτό το λόγο, δεν είναι εμφανής καμία υπογραφή ή αλλοίωση στη συνηθισμένη κίνηση (traffic) του δικτύου, γεγονός που ενδεχομένως θα μαρτυρούσε ότι στο μηχάνημα τρέχει ένα packet sniffer. Ωστόσο, υπάρχουν τρόποι ώστε να γίνονται φανερές network interfaces στο δίκτυο, οι οποίες βρίσκονται σε promiscuous mode, και αυτό να χρησιμοποιηθεί για εντοπισμό μη εγκεκριμένων packet sniffers. Οι κυριότερες μέθοδοι που χρησιμοποιούνται για το σκοπό αυτό είναι:

- Μέθοδος του Ping (Ping method)
- Μέθοδος ARP (ARP method)
- Εξέταση localhost
- Μέθοδος λανθάνουσας κατάστασης (latency method)

4.1.0.3 Δίκτυα με switch

Ένα άλλο σημείο άξιο προσοχής, είναι η χρήση switch (μεταγωγέων), αντί για hub (διανομείς), σε ένα δίκτυο. Τα πακέτα που φθάνουν σε μια inteface (επιφάνεια διεπαφής) του switch δεν στέλνονται σε κάθε άλλη interface του. Για αυτό το λόγο, ένα δίκτυο που χρησιμοποιεί κυρίως switch, αντί για ένα περιβάλλον γεμάτο με hub (ένας τομέας), έχει μεγαλύτερες πιθανότητες να αχρηστεύσει ένα packet sniffer.

Από την άλλη πλευρά όμως ούτε ένα switch είναι άτρωτο απέναντι σε ένα packet sniffer. Συγκεκριμένα:

- Εφαρμόζοντας μια παραβίαση που αποκαλείται ARP poisoning, στην ουσία το switch "ξεγελιέται" ώστε να αντικαταστήσει το μηχάνημα στο οποίο τρέχει το packet sniffer με το μηχάνημα-προορισμό. Αφού συλληφθούν τα δεδομένα, τα πακέτα μπορούν να σταλθούν στον πραγματικό προορισμό.

- Μία άλλη τεχνική είναι να "γεμίσει" κάποιος (flood) το switch με διευθύνσεις MAC. Με αυτόν τον τρόπο το switch εμπίπτει σε έναν ειδικό τρόπο λειτουργίας, που αποκαλείται failopen mode. Σε αυτόν τον τρόπο λειτουργίας ένα switch αρχίζει να συμπεριφέρεται ως hub, μεταδίδοντας όλα τα πακέτα σε όλα τα μηχανήματα ώστε να είναι σίγουρο πως τα πακέτα θα φτάσουν στον προορισμό τους.

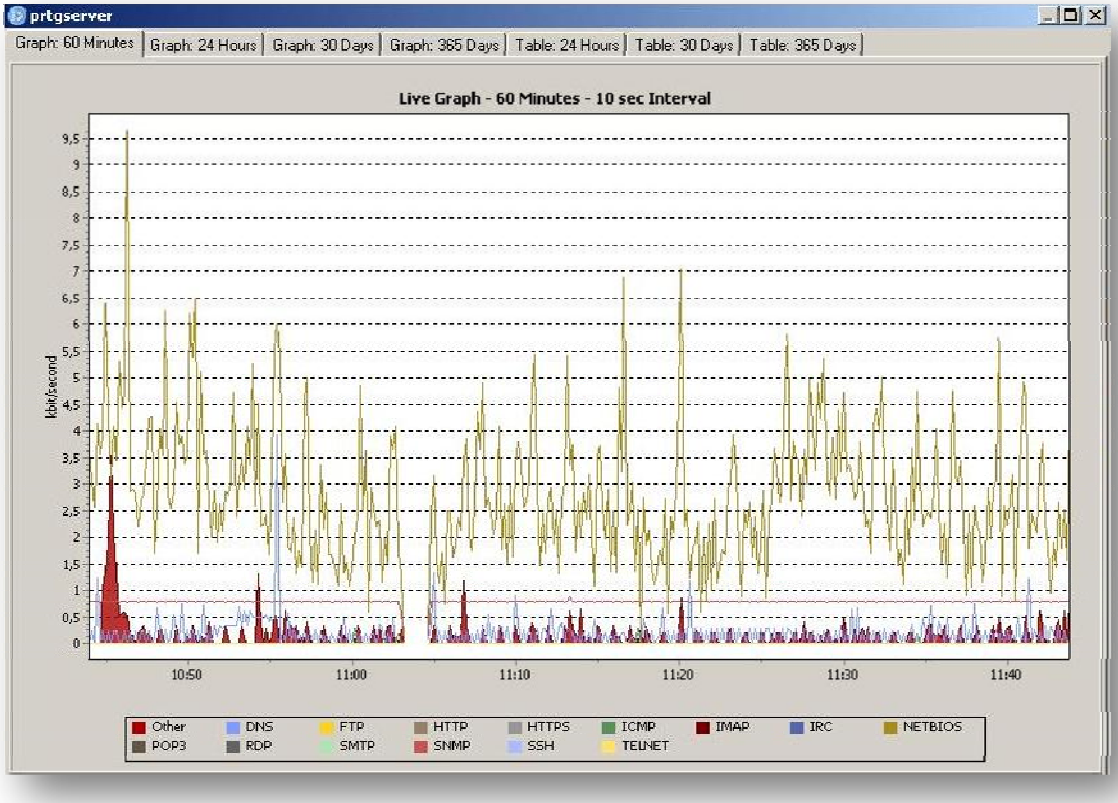
Παρόλα αυτά και οι δύο τεχνικές (ARP poisoning και MAC flooding δημιουργούν υπογραφές που είναι ανιχνεύσιμες από προγράμματα τα οποία εντοπίζουν packet sniffers.

4.1.0.4 Κρυπτογράφηση

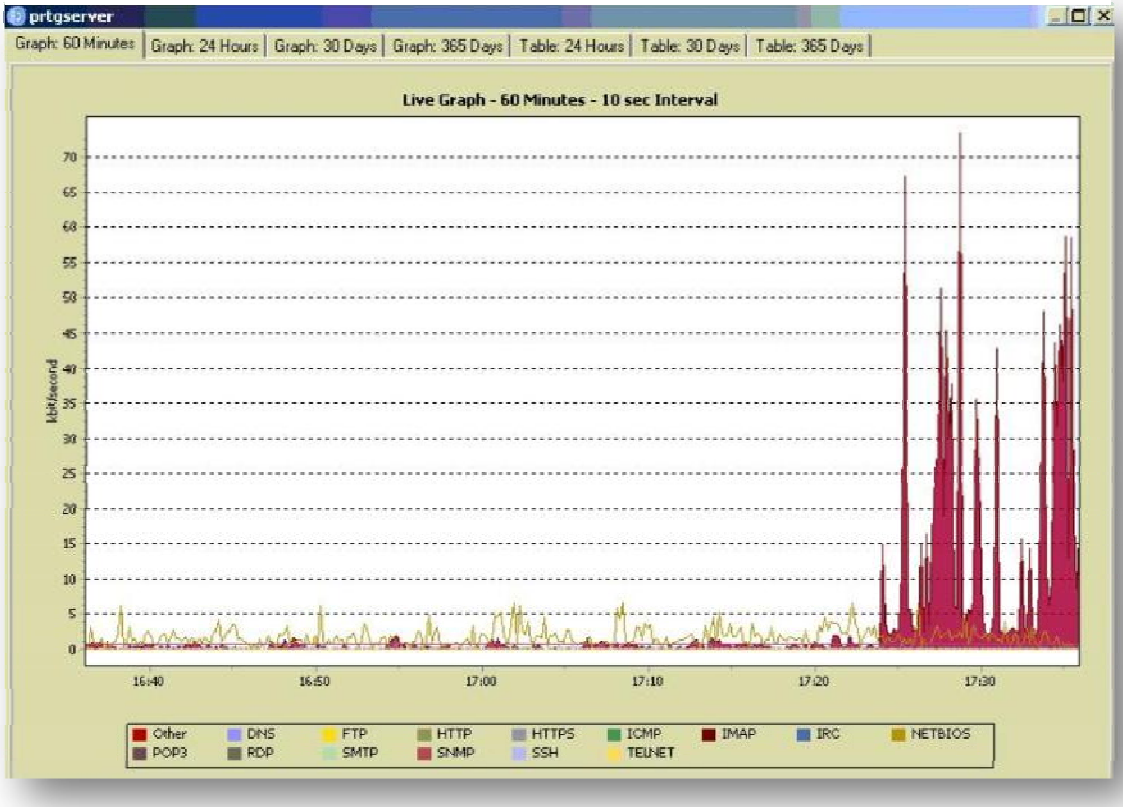
Ο καλύτερος τρόπος άμυνας απέναντι σε ένα packet sniffer είναι η χρήση κρυπτογράφησης. Η ιδιαίτερα ισχυρή κρυπτογράφηση αχρηστεύει το sniffer, αφού τα συλληφθέντα πακέτα δεν μπορούν να αποκωδικοποιηθούν, ώστε να διαβαστούν οι πληροφορίες που περιέχουν. Η κρυπτογράφηση μπορεί να γίνει σε αρκετές υπηρεσίες (services) με τη χρήση ανάλογων πρωτοκόλλων όπως πχ. SSL, PGP, SSH κ.α.

4.1.1 Μετρήσεις Packet Sniffer (Γραφική Απεικόνιση)

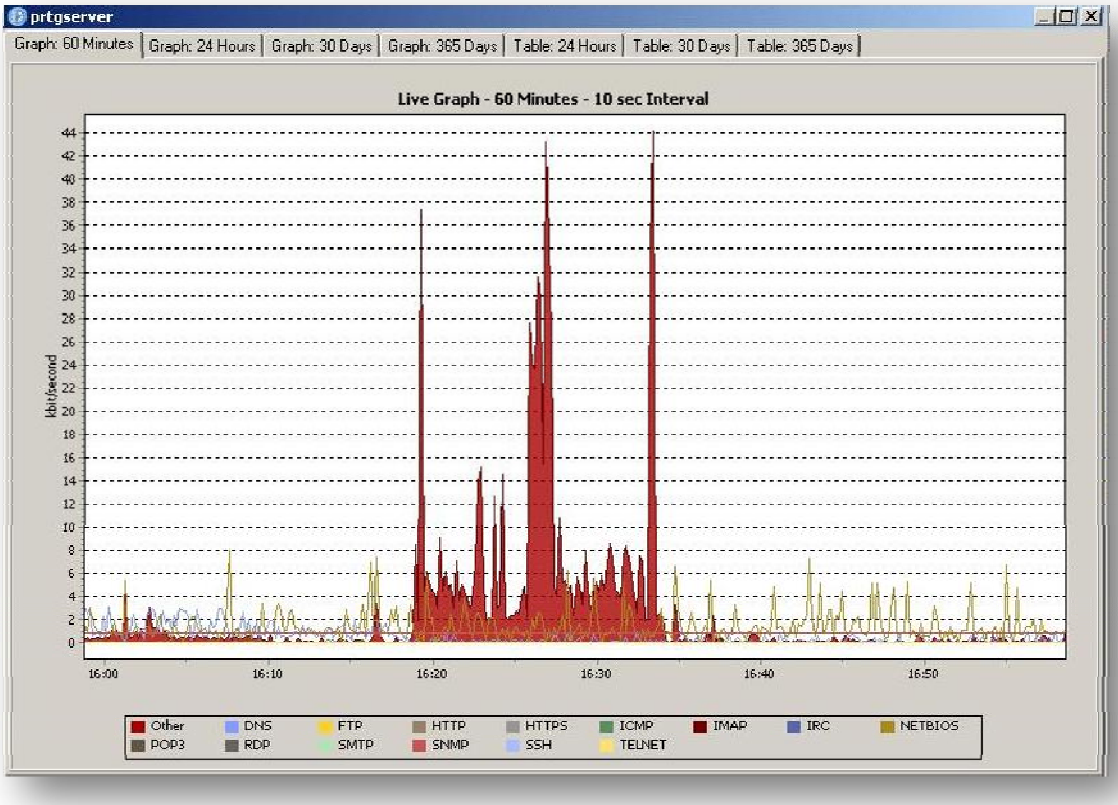
4.1.1.1 Ωριαίες μετρήσεις



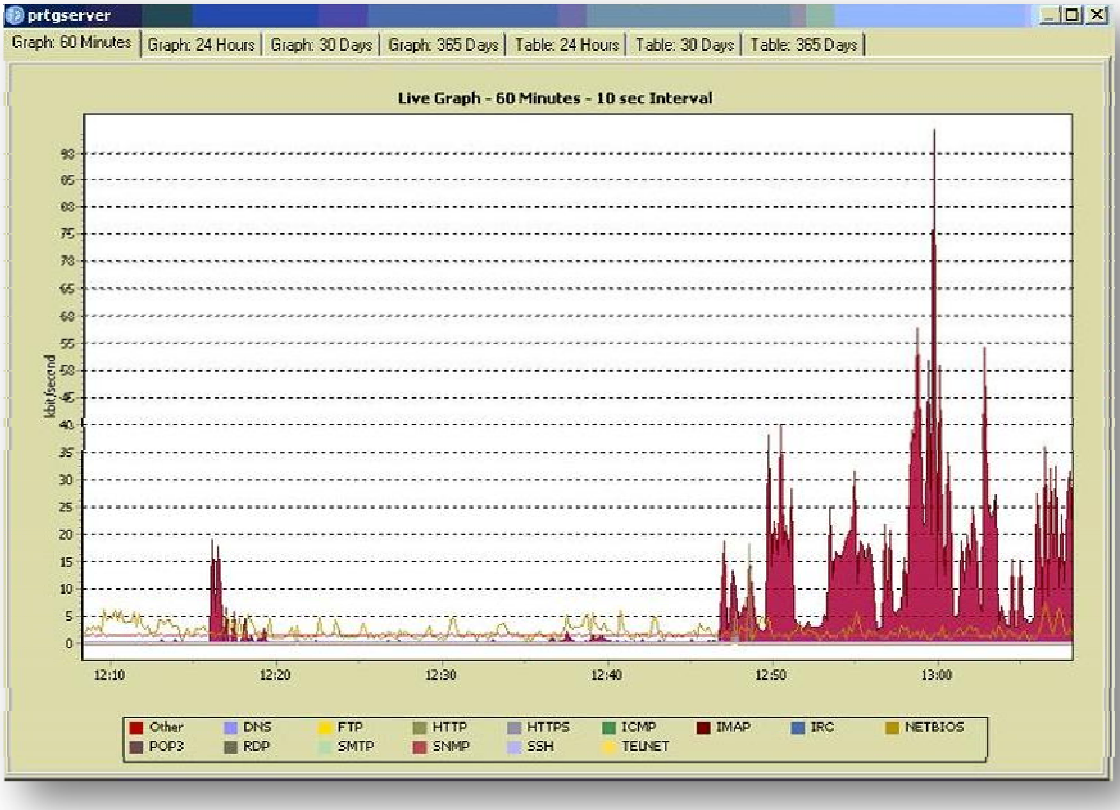
Εικόνα 31.Ωριαία μέτρηση με εμφάνιση του πρωτοκόλλου HTTP



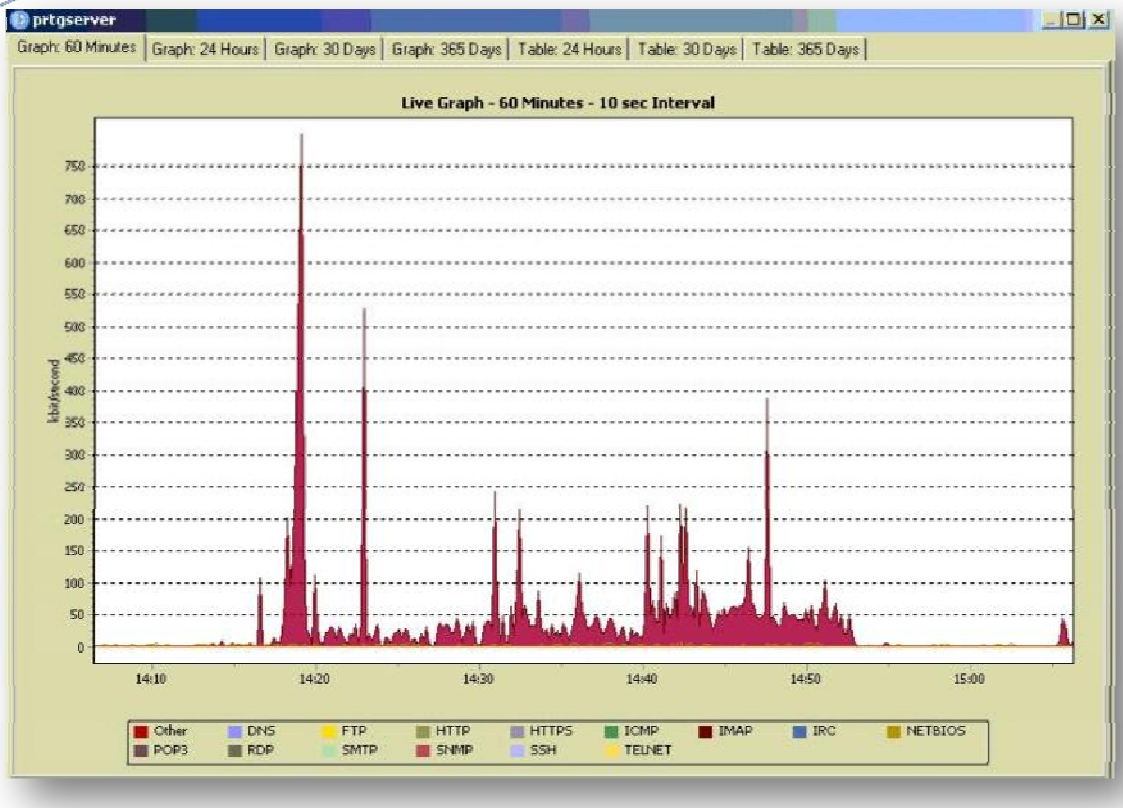
Εικόνα 32. Ωριαία μέτρηση



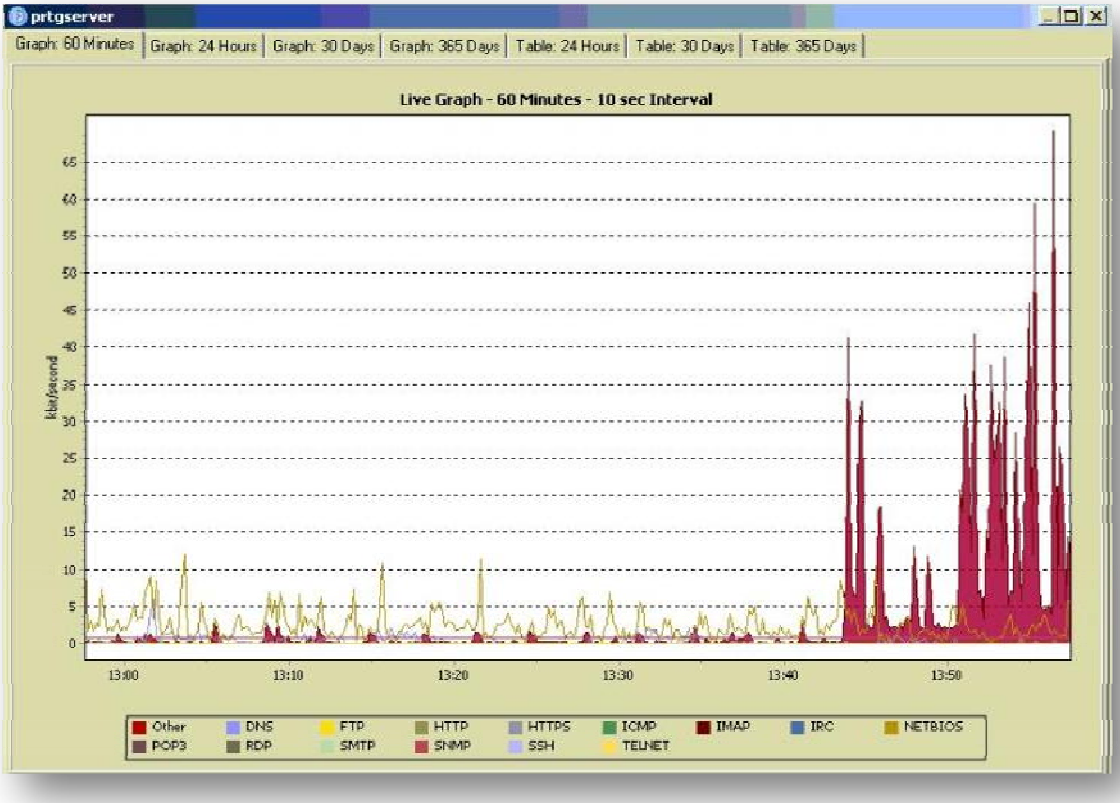
Εικόνα 33



Εικόνα 34

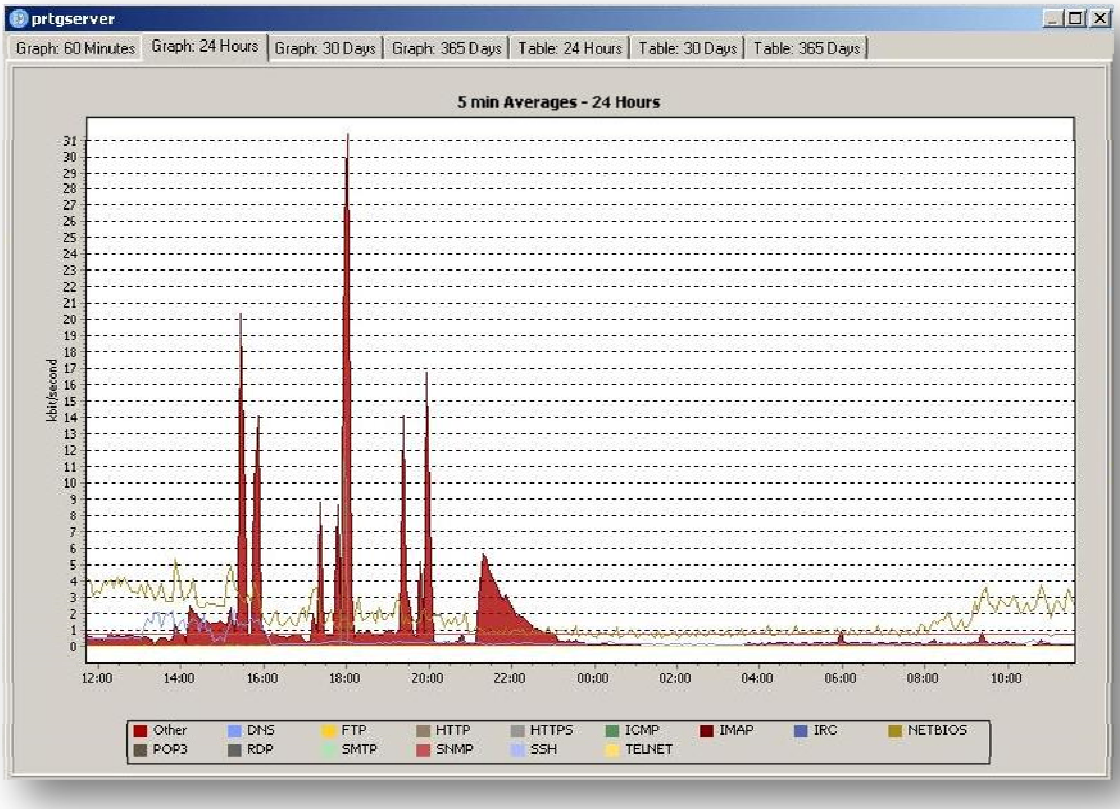


Εικόνα 35

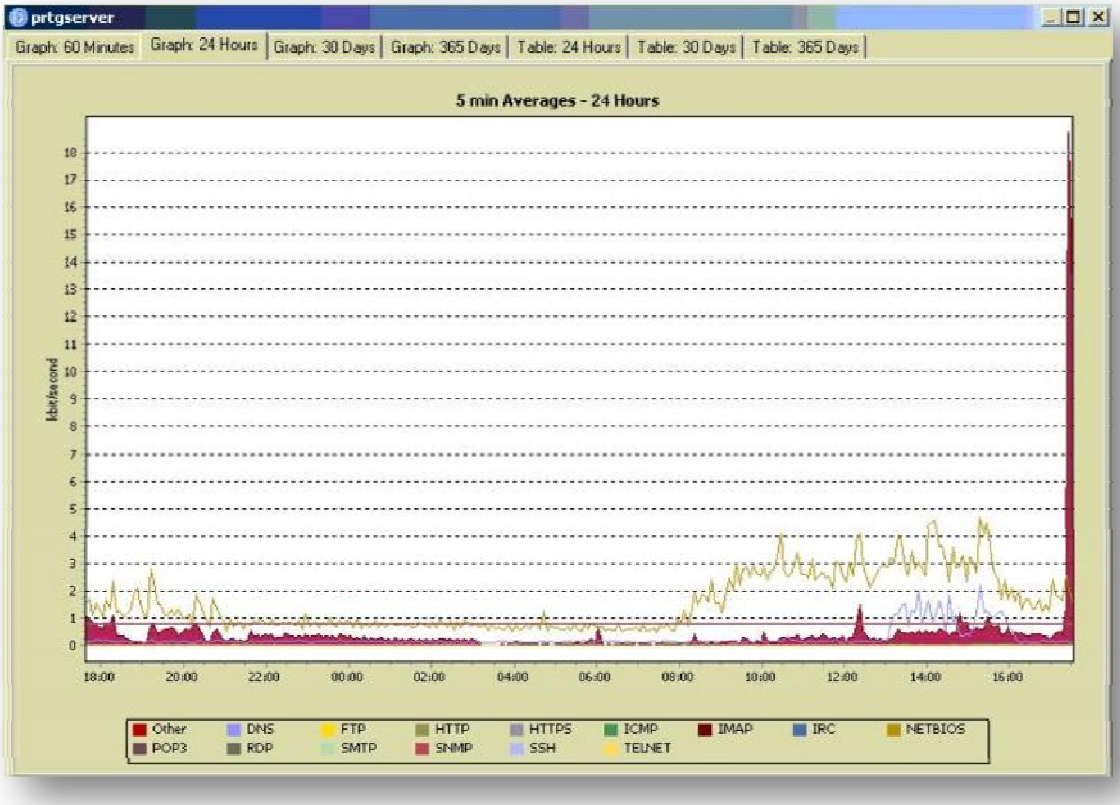


Εικόνα 36

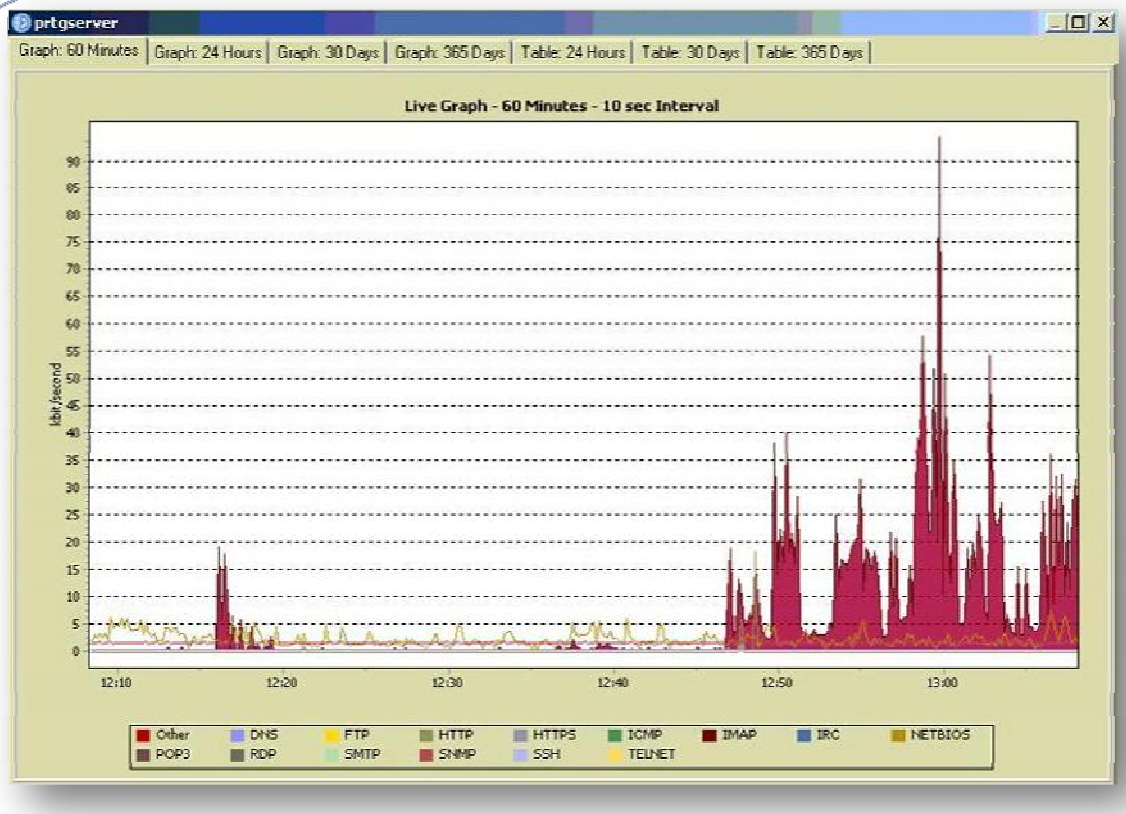
4.1.1.2 Ημερήσιες μετρήσεις



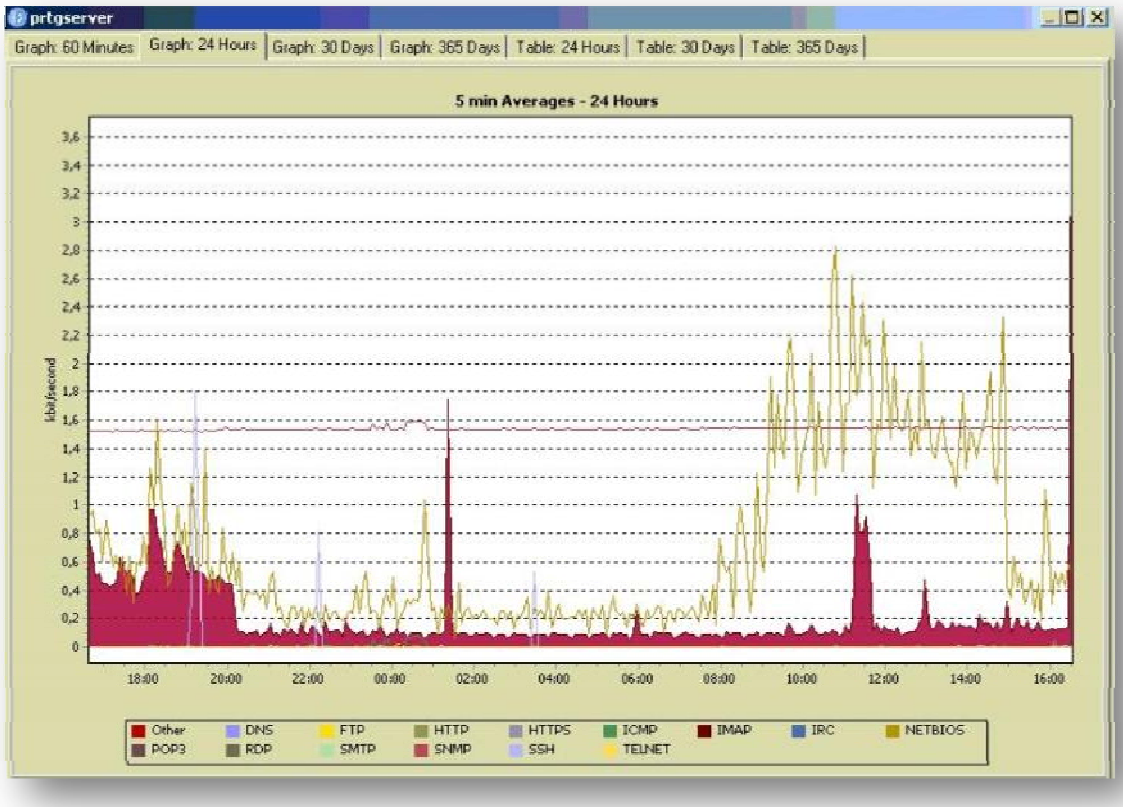
Εικόνα 37



Εικόνα 38

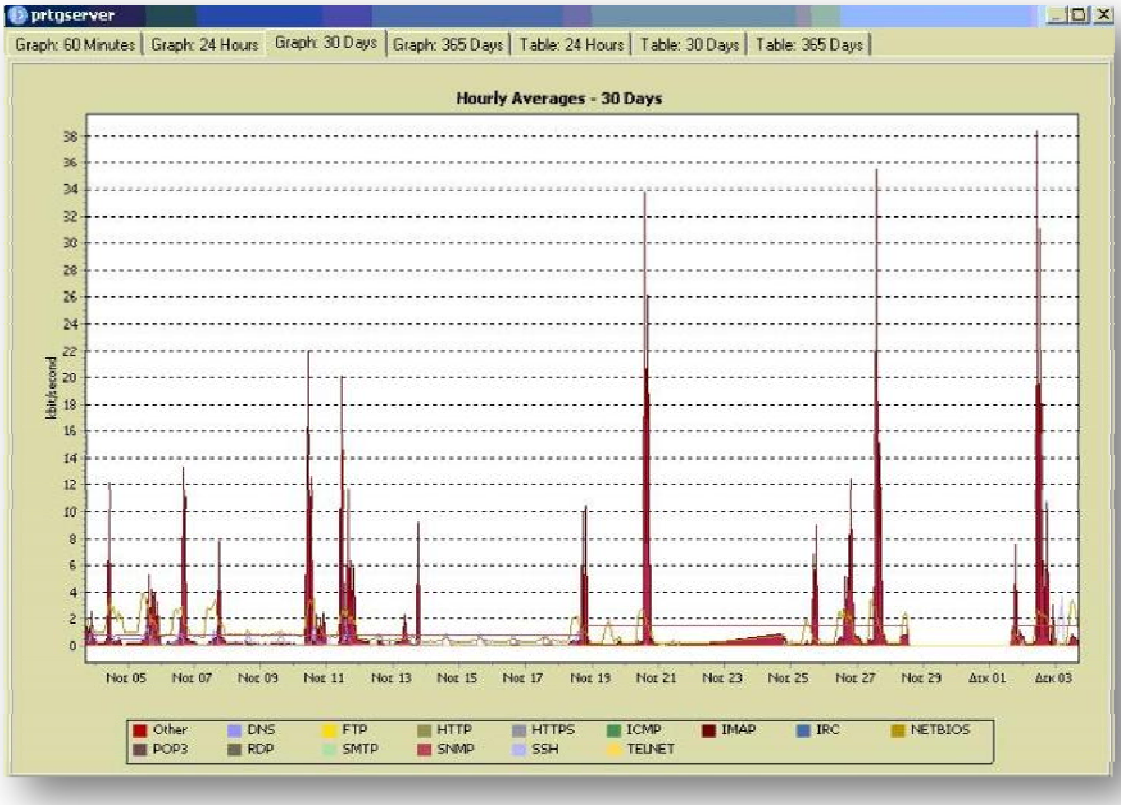


Εικόνα 39

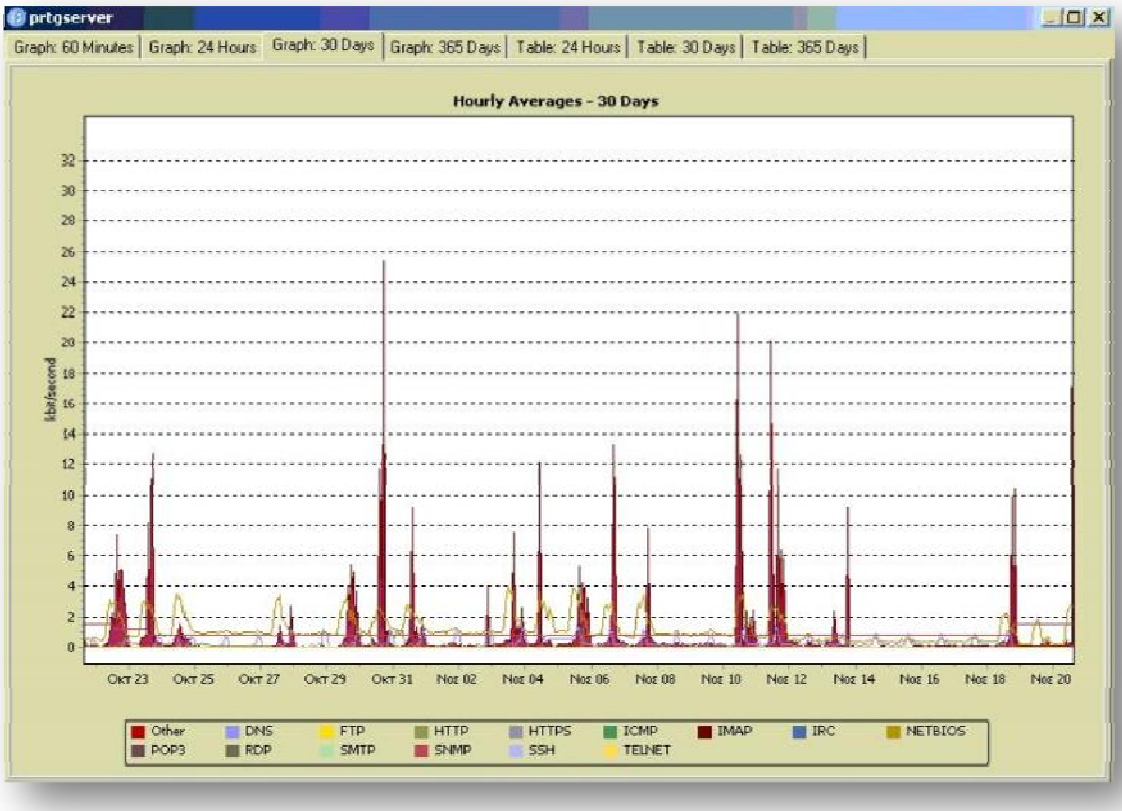


Εικόνα 40

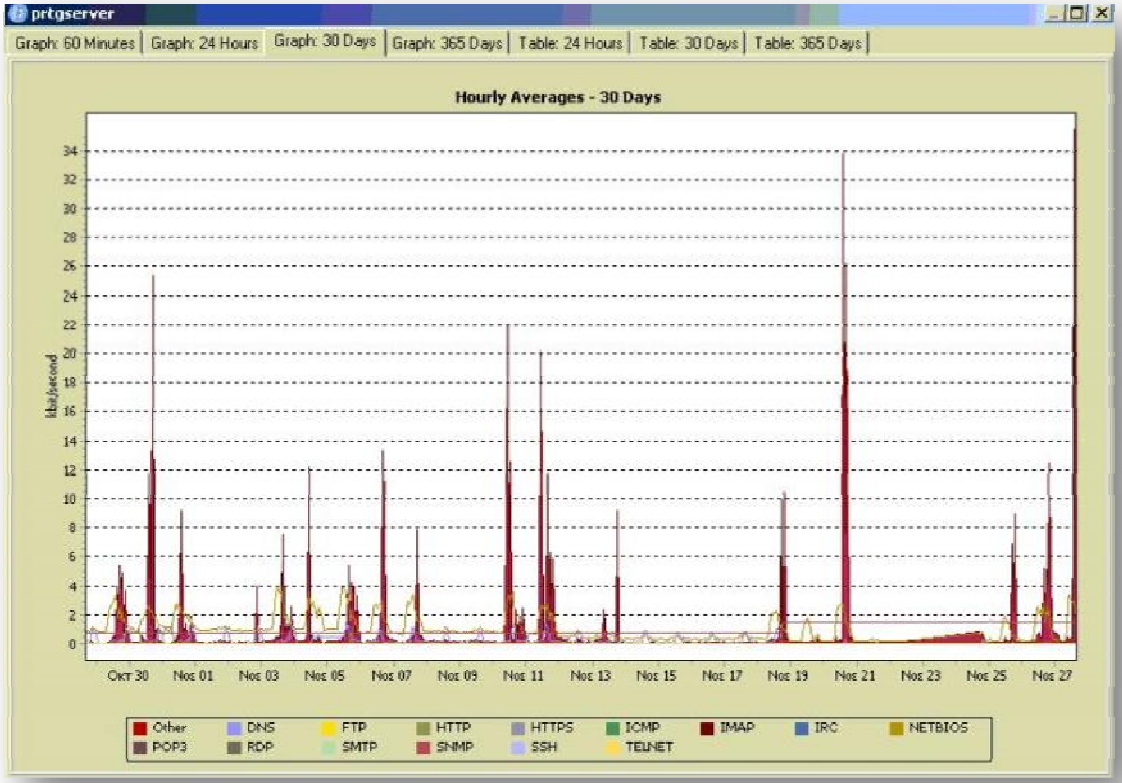
4.1.1.3 Μηνιαίες μετρήσεις



Εικόνα 41



Εικόνα 42


prtgserver
Graph: 60 Minutes
Graph: 24 Hours
Graph: 30 Days
Graph: 365 Days
Table: 24 Hours
Table: 30 Days
Table: 365 Days
Hourly Averages - 30 Days
kbit/second
34
32
30
28
26
24
22
20
18
16
14
12
10
8
6
4
2
0
Οκτ 30
Νοε 01
Νοε 03
Νοε 05
Νοε 07
Νοε 09
Νοε 11
Νοε 13
Νοε 15
Νοε 17
Νοε 19
Νοε 21
Νοε 23
Νοε 25
Νοε 27
Other
DNS
FTP
HTTP
HTTPS
ICMP
IMAP
IRC
NETBIOS
POP3
RDP
SMTP
SNMP
SSH
TELNET

Εικόνα 43

4.2 Top Protocols

4.2.1 HTTP

Στις αρχές τις δεκαετίας του 1980 το Διαδίκτυο χρησιμοποιούνταν κυρίως στην ακαδημαϊκή κοινότητα. Οι υπηρεσίες που παρείχε ήταν η πρόσβαση σε έναν απομακρυσμένο υπολογιστή, το ηλεκτρονικό ταχυδρομείο, η μεταφορά αρχείων και η αποστολή και λήψη νέων. Το 1989 στα εργαστήρια του Ευρωπαϊκού Κέντρου Πυρηνικών Ερευνών CERN προτάθηκε η ιδέα του Παγκόσμιου Ιστού (World Wide Web – WWW) ή απλά Ιστού (Web) από τον φυσικό Tim Berners – Lee ως μία αρχιτεκτονική για την επικοινωνία μεταξύ των διαφόρων ερευνητικών ομάδων του CERN. Η βασική ιδέα της αρχιτεκτονικής αυτής ήταν η διασύνδεση των εγγράφων που ήταν διασκορπισμένα στο Διαδίκτυο. Γρήγορα έγινε ιδιαίτερα δημοφιλές και γύρω του αναπτύχθηκε μία ολόκληρη βιομηχανία. Η δημοτικότητά του οφείλεται τόσο στο γραφικό περιβάλλον χρήσης του όσο και στην μεγάλη πληθώρα πληροφοριών που διαθέτει με αποτέλεσμα ο κάθε χρήστης να μπορεί να βρει αυτό που τον ενδιαφέρει με ελάχιστο κόστος.

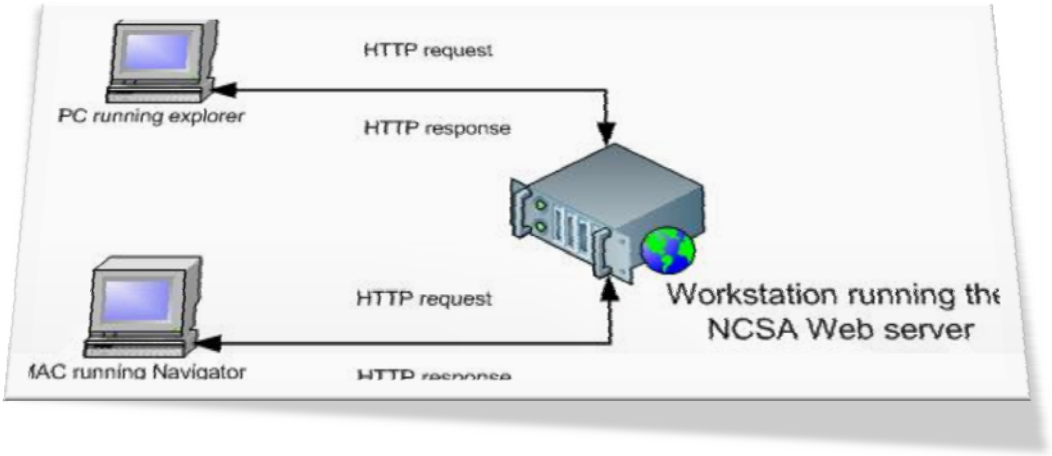
Το Πρωτόκολλο Μεταφοράς Υπερκειμένου HTTP (HyperText Transfer Protocol) είναι η καρδιά του Ιστού. Το HTTP ανήκει στο στρώμα εφαρμογών του Διαδικτύου και υλοποιείτε ως δύο προγράμματα: ένα πρόγραμμα πελάτη (client program) και ένα πρόγραμμα εξυπηρετητή (server program). Τα δύο αυτά προγράμματα εκτελούνται σε διαφορετικά μηχανήματα επικοινωνώντας μεταξύ τους ανταλλάσσοντας HTTP μηνύματα. Συγκεκριμένα το HTTP ορίζει τη δομή των μηνυμάτων αυτών καθώς και τον τρόπο ανταλλαγής τους ανάμεσα στον πελάτη και στον εξυπηρετητή.

Πριν περιγράψουμε αναλυτικά το πρωτόκολλο HTTP πρέπει να αναφερθούμε σε κάποια βασική ορολογία του Ιστού. Μία Ιστοσελίδα (Web page) αποτελείται από αντικείμενα. Με τον όρο αντικείμενο (object) εννοούμε ένα απλό αρχείο, όπως ένα αρχείο HTML, ένα αρχείο εικόνας ή ένα αρχείο βίντεο, το οποίο μπορεί να προσπελαστεί μέσω ενός URL. Οι περισσότερες Ιστοσελίδες αποτελούνται από ένα βασικό αρχείο HTML και διάφορα σχετικά αντικείμενα. Αν υποθέσουμε ότι έχουμε μία Ιστοσελίδα που περιέχει ένα αρχείο HTML και 3 αρχεία εικόνων τότε λέμε ότι η Ιστοσελίδα έχει 4 αντικείμενα. Το βασικό αρχείο HTML αναφέρεται στα άλλα αντικείμενα της σελίδας μέσω των URL των αντικειμένων. Κάθε URL αποτελείται από δύο

τμήματα: το όνομα του υπολογιστή – host στον οποίον είναι αποθηκευμένο το αρχείο και το όνομα του μονοπατιού (path) του αντικειμένου. Π.χ. το URL www.ntua.gr/index.htm έχει ως όνομα host το www.ntua.gr και ως όνομα μονοπατιού το index.htm.

Ο browser είναι ο αντιπρόσωπος του Ιστού: απεικονίζει στον χρήστη τη ζητούμενη Ιστοσελίδα και παρέχει πληθώρα χαρακτηριστικών πλοήγησης και παραμετροποίησης. Επίσης, στους browser υλοποιείτε και η πλευρά του πελάτη του πρωτοκόλλου HTTP. Ένας εξυπηρετητής Ιστού (Web server) αποθηκεύει τα αντικείμενα της Ιστοσελίδας, το καθένα από τα οποία έχει ως διεύθυνση ένα URL. Στους εξυπηρετητές Ιστού υλοποιείτε και η πλευρά του εξυπηρετητή του πρωτοκόλλου HTTP.

Το HTTP ορίζει τον τρόπο με τον οποίο οι πελάτες του Ιστού (π.χ. οι browsers) ζητούν (request) Ιστοσελίδες από τους εξυπηρετητές του Ιστού (π.χ. τους Web servers) και πως οι εξυπηρετητές μεταφέρουν τις Ιστοσελίδες στους πελάτες. Η βασική ιδέα της του πρωτοκόλλου αυτού φαίνεται στο παρακάτω σχήμα.



Εικόνα 44

Όταν ο χρήστης ζητά μία Ιστοσελίδα, ο browser στέλνει ένα μήνυμα **HTTP αίτησης (HTTP request)**, για τα διάφορα αντικείμενα της σελίδας, στον εξυπηρετητή. Ο εξυπηρετητής όταν λάβει το μήνυμα αυτό ανταποκρίνεται με μηνύματα **HTTP απόκρισης (HTTP response)** στα οποία περιέχονται τα αιτούμενα αντικείμενα. Μέχρι το 1997 όλοι οι browsers και όλοι οι εξυπηρετητές Ιστού υλοποιούσαν την έκδοση 1.0 του HTTP, που για συντομία γράφεται **HTTP/1.0**. Από το 1998 όμως άρχισαν να υποστηρίζουν και το **HTTP/1.1**, το οποίο είναι συμβατό με το HTTP/1.0. Δηλαδή, ένας browser που υποστηρίζει το HTTP/1.0 μπορεί να επικοινωνήσει με ένας

εξυπηρετητή Ιστού που υποστηρίζει το HTTP/1.1 και, αντιστρόφως, ένας browser που υποστηρίζει το HTTP/1.1 μπορεί να επικοινωνήσει με έναν εξυπηρετητή Ιστού που υποστηρίζει το HTTP/1.0.

Τόσο το HTTP/1.0 όσο και το HTTP/1.1 χρησιμοποιούν το **TCP** ως πρωτόκολλο μεταφοράς. Αφού ο πελάτης εγκαταστήσει μία σύνδεση TCP με τον εξυπηρετητή αρχίζει την αποστολή μηνυμάτων – αιτήσεων προς αυτόν και τη λήψη μηνυμάτων – αποκρίσεων από αυτόν. Λόγω της χρήσης του TCP το HTTP δεν χρειάζεται να ασχοληθεί καθόλου με τη μεταφορά των δεδομένων. Το μόνο που πρέπει να κάνει είναι να στείλει τις αιτήσεις μέσω της TCP σύνδεσης και να περιμένει τις αποκρίσεις. Το TCP εγγυάται την αξιόπιστη μεταφορά των δεδομένων καθώς και τον έλεγχο της συμφόρησης.

Οι εξυπηρετητές του HTTP δεν κρατάνε καθόλου στοιχεία για την κατάσταση του πελάτη. Επομένως, αν ένας πελάτης στείλει μία αίτηση για ένα αρχείο δύο φορές, ο εξυπηρετητής θα του στείλει το αρχείο αυτό δύο φορές. Τα πρωτόκολλα που δεν κρατάνε καθόλου πληροφορία για την κατάσταση του πελάτη ονομάζονται stateless.

4.2.2 SNMP

Πρωτόκολλο Διαχείρισης Δικτύου : (SNMP). Το SNMP σχεδιάστηκε ώστε να επιτρέπει στο διαχειριστή δικτύου να παρακολουθεί όλες τις συσκευές του δικτύου από ένα μόνο σημείο , ακόμη και αν αυτές είναι διασκορπισμένες σε όλο τον κόσμο. Το SNMP είναι στην ουσία μια τυποποιημένη γλώσσα που επιτρέπει να παρακολουθούνται συσκευές δικτύου , διαφορετικού τύπου , μέσα από ένα σύστημα διαχείρισης. Χρησιμοποιώντας το πρωτόκολλο SNMP και ένα ***Σταθμό Διαχείρισης Δικτύου*** **: (NMS)** , ο διαχειριστής του δικτύου μπορεί να παρακολουθεί και να ελέγχει διάφορες παραμέτρους των συσκευών.

Η στρατηγική του SNMP είναι ότι η παρακολούθηση της κατάστασης του δικτύου επιτυγχάνεται με το (NMS) από ένα μόνο σημείο. Ο σταθμός διαχείρισης (NMS) επικοινωνεί με ένα στοιχείο του δικτύου (π.χ. gateway , router , UPS , κ.λπ.) είτε για να λάβει πληροφορίες (διαδικασία που ονομάζεται "get") ή για να τροποποιήσει κάποια παράμετρο της λειτουργίας του (διαδικασία που ονομάζεται "set"). Κά-

ποιο στοιχείο του δικτύου επικοινωνεί αυτόματα με έναν σταθμό διαχείρισης όταν κάτι ασυνήθιστο συμβαίνει. Κάτω από την εποπτεία του SNMP εκδίδονται μηνύματα που αναφέρουν την κατάσταση που βρίσκεται κάποιο στοιχείο. Το σύνολο αυτών των μηνυμάτων περιγράφει την κατάσταση που βρίσκεται όλο το δίκτυο.

Μια SNMP λειτουργία λαμβάνει τη μορφή ενός πρωτοκόλλου Data Unit (PDU), κατά βάση ένα φανταχτερό λέξη για πακέτα. Έκδοση 1 SNMP υποστηρίζει πέντε πιθανές PDUs:

- **GetRequest / SetRequest** προμήθειες κατάλογο των αντικειμένων και, ενδεχομένως, τις αξίες, πρέπει να οριστεί σε (SetRequest). Σε κάθε περίπτωση, το γραφείο επιστρέφει μια GetResponse.

- **GetResponse** ενημερώνει το σταθμό διαχείρισης των αποτελεσμάτων μιας GetRequest ή SetRequest επιστρέφοντας ένα λάθος ένδειξη, καθώς και τον κατάλογο των μεταβλητών / παγιοποιήσεων αξία.

- **GetNextRequest** χρησιμοποιείται για την εκτέλεση πίνακα εγκάρσια, και σε άλλες περιπτώσεις όπου η διαχείριση των σταθμών δεν γνωρίζει την ακριβή MIB όνομα του αντικειμένου το επιθυμεί. GetNextRequest δεν απαιτεί την ακριβή ονομασία που θα καθορίζεται? Αν δεν υπάρχει αντικείμενο της καθορισμένης όνομα, το επόμενο αντικείμενο των MIB επιστρέφεται. Σημειώνεται ότι για την υποστήριξη αυτής, πρέπει να είναι αυστηρά MIBs διέταξε σετ (και είναι).

- **Παγίδα** είναι το μόνο PDU που αποστέλλονται από έναν πράκτορα με δική της πρωτοβουλία. Έχει χρησιμοποιηθεί για να κοινοποιήσουν τη διαχείριση του σταθμού μια ασυνήθιστη περίπτωση κατά την οποία μπορεί να ζητήσει περαιτέρω προσοχή (όπως η σύνδεση θα τα κάτω). Στην έκδοση 2, οι παγίδες που κατονομάζονται στην MIB χώρο. Νεότερο MIBs διευκρινίζει ότι ο έλεγχος της διαχείρισης αντικείμενα πώς οι παγίδες αποσταλεί.

SNMP Εκδόσεις

Το πρωτόκολλο SNMP έχει ωφεληθεί από σημαντικές αναβαθμίσεις από την εισαγωγή του το 1988. Δυστυχώς, ένα μεγάλο ποσοστό του δικτύου πωλητών στοιχείο και μάλιστα ορισμένοι πωλητές συστημάτων διαχείρισης δικτύου δεν επωφελούνται από αυτές τις βελτιώσεις. Πολλά στοιχεία του δικτύου υποστήριξης μόνο SNMPv1 και SNMPv2c. Υποστήριξη για SNMPv3 είναι ελάχιστη.

Έκδοση	Περιγραφή
SNMPv1	SNMPv1, η οποία θέτει σε εφαρμογή κοινοτικής βάσης ασφαλείας
SNMPv2c	SNMPv2 κοινότητας με βάση την ασφάλεια
SNMPv2u	SNMPv2 χρήστη με βάση την ασφάλεια
SNMPv2	SNMPv2 μέρος με βάση την ασφάλεια
SNMPv3	SNMPv3, η οποία θέτει σε εφαρμογή το χρήστη με βάση την ασφάλεια

4.2.3 POP3

Πρωτόκολλο POP3 : Το πρωτόκολλο POP3 είναι ένα απλό πρωτόκολλο μεταφοράς, με περιορισμένες δυνατότητες. Το πρωτόκολλο αυτό ξεκινά όταν ο αντιπρόσωπος χρήστη δημιουργεί μία TCP σύνδεση στη θύρα 110 του μοιραζόμενου εξυπηρετητή ταχυδρομείου και έχει τρεις φάσεις: πιστοποίηση (authentication), συναλλαγή (transaction) και ενημέρωση (update). Κατά την πρώτη φάση ο αντιπρόσωπος χρήστη στέλνει ένα όνομα χρήστη (username) και έναν κωδικό (password) στον εξυπηρετητή, τα οποία χρησιμοποιούνται από τον εξυπηρετητή για την πιστοποίηση του χρήστη. Κατά τη δεύτερη φάση, ο αντιπρόσωπος χρήστη μπορεί να σημειώσει τα μηνύματα προς διαγραφή ή να αφαιρέσει τα σημάδια διαγραφής από κάποια μηνύματα και να πάρει στατιστικά στοιχεία για τη χρήση του Ηλεκτρονικού Ταχυδρομείου. Κατά την τρίτη φάση, που εκτελείτε όταν ο χρήστης δώσει την εντολή quit, για τον τερματισμό του πρωτοκόλλου POP3, διαγράφονται τα μηνύματα που είναι σημειωμένα για διαγραφή.

Στη φάση της POP3 συναλλαγής, ο χρήστης δίνει εντολές στις οποίες ο εξυπηρετητής στέλνει αποκρίσεις (responses). Υπάρχουν δύο ειδών αποκρίσεων: +OK (που μερικές φορές ακολουθείται από δεδομένα από τον εξυπηρετητή προς τον πελάτη) για να δηλώσει ο εξυπηρετητής ότι η προηγουμένη εντολή ήταν έγκυρη, και –ERR για να δηλωθεί ότι η προηγούμενη εντολή είχε κάποιο λάθος.

Η φάση της πιστοποίησης έχει δύο κύριες εντολές: user <username> και pass <password>. Αν το password δεν αντιστοιχεί στο υπαρκτό username τότε ο εξυπηρετητής αποκρίνεται με ένα μήνυμα –ERR, διαφορετικά αποκρίνεται με ένα μήνυμα OK. Ακολουθεί ένα παράδειγμα επιτυχούς πιστοποίησης.

4.2.4 DNS (Domain Name System).

Το πρωτόκολλο DNS : (Domain Name System). Κάθε μηχάνημα – host του Διαδικτύου μπορεί να αναγνωριστεί από την IP διεύθυνσή του, που είναι ένας δυαδικός αριθμός των 32 bits. Το ίδιο το δίκτυο (και συγκεκριμένα το στρώμα διαδικτύου) καταλαβαίνει μόνο τις IP διευθύνσεις. Οι άνθρωποι, όμως, μπορούν πιο εύκολα να θυμούνται ονόματα και όχι δυαδικά νούμερα. Για αυτό το λόγο τις περισσότερες φορές τα προγράμματα σπάνια απευθύνονται στους host του Διαδικτύου χρησιμοποιώντας την IP διεύθυνση, αλλά κάνουν χρήση συμβολικών ονομάτων, με την μορφή ακολουθιών ASCII χαρακτήρων. Για την αντιστοίχηση μεταξύ των δυαδικών διευθύνσεων και των διευθύνσεων σε μορφή ASCII χαρακτήρων χρησιμοποιείται ένα πρωτόκολλο του στρώματος εφαρμογών, το DNS (Domain Name System).

Το DNS είναι μία κατανεμημένη βάση δεδομένων που υλοποιείται μέσω μίας ιεραρχίας εξυπηρετητών ονομάτων (name servers) και ένα πρωτόκολλο του στρώματος εφαρμογής που επιτρέπει στους host και στους εξυπηρετητές ονομάτων να επικοινωνούν για τους σκοπούς της υπηρεσίας μετάφρασης των διαφορετικών μορφών διευθύνσεων. Το πρωτόκολλο DNS χρησιμοποιεί το UDP και συγκεκριμένα την θύρα 53.

Το DNS χρησιμοποιείται συχνά από άλλα πρωτόκολλα του στρώματος εφαρμογών, όπως το HTTP και το FTP, για την μετάφραση των διευθύνσεων που δίνουν οι χρήστες σε IP διευθύνσεις. Έστω ότι ένας χρήστης ζητά από τον browser να εμφανιστεί η σελίδα που έχει ως URL το http://www.ntua.gr/index.htm. Για να μπο-

ρέσει το μηχάνημα του χρήστη να στείλει μία HTTP αίτηση στον εξυπηρετητή Ιστού (Web server) www.ntua.gr, το μηχάνημα του χρήστη πρέπει να μάθει την IP διεύθυνση του www.ntua.gr. Αυτό συμβαίνει ως εξής: στο μηχάνημα του χρήστη, που λειτουργεί ως DNS πελάτης, ο browser αποσπά από το URL και περνά το www.ntua.gr στον DNS πελάτη. Ως μέρος της DNS ερώτησης (query) ο DNS πελάτης στέλνει το όνομα του host στον DNS εξυπηρετητή, από τον οποίο λαμβάνει μία απάντηση (reply) που περιλαμβάνει την IP διεύθυνση του host. Στη συνέχεια ο browser ανοίγει μία σύνδεση TCP με τον εξυπηρετητή HTTP που βρίσκεται στην συγκεκριμένη διεύθυνση IP. Όλα τα πακέτα IP (datagrams) που στέλνονται από τον πελάτη προς τον εξυπηρετητή για την συγκεκριμένη σύνδεση (δηλαδή όλες οι αιτήσεις HTTP) έχουν ως διεύθυνση προορισμού αυτή την διεύθυνση IP. Από το παράδειγμα αυτό γίνεται φανερό ότι το DNS εισάγει μία επιπλέον καθυστέρηση στις εφαρμογές του Διαδικτύου που χρησιμοποιούν το DNS. Για τη μείωση της καθυστέρησης αυτής η επιθυμητή διεύθυνση IP συνήθως αποθηκεύεται προσωρινά σε κάποιον κοντινό εξυπηρετητή ονομάτων, ο οποίος βοηθά στην μείωση του φορτίου στο ίδιο το Διαδίκτυο αλλά και στην μείωση της μέσης καθυστέρησης.

Όπως αναφέρθηκε και παραπάνω, το DNS ανήκει στο στρώμα εφαρμογών του Διαδικτύου. Σε σχέση όμως με τα άλλα πρωτόκολλα του στρώματος εφαρμογών, όπως το FTP και το HTTP, το DNS έχει μία σημαντική διαφορά: ο χρήστης δεν μπορεί να έρθει σε απευθείας επαφή με το DNS, αλλά αντίθετα το DNS παρέχει μία σημαντική λειτουργία του Διαδικτύου, την μετάφραση μεταξύ των ονομάτων των host και των διευθύνσεων IP, στις εφαρμογές των χρηστών και του άλλου λογισμικού του Διαδικτύου.

Αν και παραπάνω αναφερθήκαμε μόνο στη μετάφραση των ονομάτων των host σε διευθύνσεις IP, το DNS παρέχει και τις ακόλουθες σημαντικές υπηρεσίες:

- **Ψευδώνυμα (Alias) Host:** Ένας host με ένα πολύπλοκο όνομα μπορεί να έχει ένα ή περισσότερα εναλλακτικά ονόματα – ψευδώνυμα, τα οποία είναι συνήθως πιο εύκολα στην απομνημόνευση. Π.χ. ένας host με όνομα hellas.core.ntua.gr μπορεί να έχει ως ψευδώνυμα τα www.ntua.gr και ntua.gr. Στην περίπτωση αυτή το όνομα hellas.core.ntua.gr λέγεται κανονικό (canonical). Το DNS μπορεί

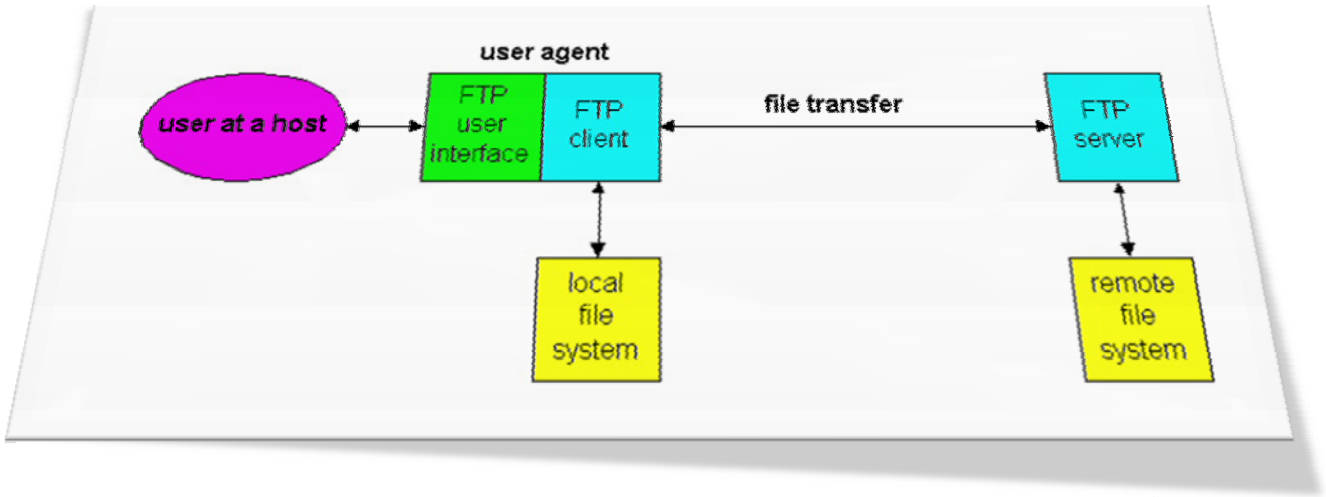
να χρησιμοποιηθεί από μία εφαρμογή για την εύρεση του κανονικού ονόματος ή της IP διεύθυνσης, δοσμένου ενός ψευδωνύμου.

- **Ψευδώνυμα Εξυπηρετητών Ταχυδρομείου:** Συχνά και τα ονόματα των διευθύνσεων του ηλεκτρονικού ταχυδρομείου (e-mail) δίνονται σε μορφή εύκολη προς απομνημόνευση. Έστω ότι ο Nick έχει έναν λογαριασμό στο yahoo.gr και η e-mail διεύθυνσή του είναι nick@yahoo.gr. Παρόλα αυτά το όνομα του host του yahoo.gr είναι πιο πολύπλοκο από το απλό yahoo.gr (π.χ. μπορεί να είναι hellas.core.yahho.gr). Το DNS στην περίπτωση αυτή χρησιμοποιείται για την εύρεση του κανονικού ονόματος για το ψευδώνυμο του host, αλλά και για την εύρεση της IP διεύθυνσης του host. Το DNS επιτρέπει να έχουν το ίδιο ψευδώνυμο τόσο ο εξυπηρετητής Ταχυδρομείου όσο και ο εξυπηρετητής Ιστού.
- **Κατανομή φορτίου:** Πολλές τοποθεσίες του Διαδικτύου έχουν πολλούς εξυπηρετητές για τον ίδιο σκοπό, π.χ. την παροχή μίας ιστοσελίδας, εξαιτίας του μεγάλου όγκου της κίνησης από και προς αυτές. Στην περίπτωση αυτή κάθε εξυπηρετητής βρίσκεται σε διαφορετικό μηχάνημα και έχει διαφορετική IP διεύθυνση. Για αυτές τις περιπτώσεις στη βάση δεδομένων του DNS περιέχονται πολλές IP διευθύνσεις με το ίδιο κανονικό όνομα. Όταν κάποιος πελάτης DNS κάνει μία επερώτηση στον DNS εξυπηρετητή για κάποιον όνομα με πολλές διευθύνσεις IP, ο DNS εξυπηρετητής ανταποκρίνεται με όλες τις διευθύνσεις IP, αλλά περιστρέφοντάς κατά μία διεύθυνση την σειρά για κάθε αίτηση που γίνεται για το συγκεκριμένο όνομα. Επειδή συνήθως οι host χρησιμοποιούν την πρώτη διεύθυνση IP που βρίσκουν στην απόκριση DNS, η περιστροφή αυτή κατανέμει το φορτίο μεταξύ των διαφόρων εξυπηρετητών.

4.2.5 FTP (File Transfer Protocol)

Πρωτόκολλο FTP : (File Transfer Protocol). Το FTP είναι ένα πρωτόκολλο που χρησιμοποιείται για την μεταφορά αρχείων από έναν υπολογιστή του Διαδικτύου σε κάποιον άλλον. Το FTP ξεκίνησε πειραματικά το 1971 αλλά παραμένει ως τις μέρες μας εξαιρετικά δημοφιλές.

Ας υποθέσουμε ότι ένας χρήστης επιθυμεί να μεταφέρει ένα ή περισσότερα αρχεία από ή προς έναν άλλο απομακρυσμένο χρήστη. Για να μπορέσει ο χρήστης να έχει πρόσβαση στα αρχεία του απομακρυσμένου υπολογιστή, δηλαδή σε κάποιο λογαριασμό (account) του απομακρυσμένου υπολογιστή, πρέπει να δώσει ένα αναγνωριστικό όνομα χρήστη (user name) και έναν κωδικό (password). Μετά την παροχή των παραπάνω πληροφοριών πιστοποίησης (authentication), ο χρήστης μπορεί να μεταφέρει αρχεία από το σύστημα αρχείων του προς το απομακρυσμένο σύστημα αρχείων, και αντιστρόφως. Όπως φαίνεται και στο παρακάτω σχήμα ο χρήστης έρχεται σε επαφή με το FTP μέσω ενός αντιπροσώπου FTP.

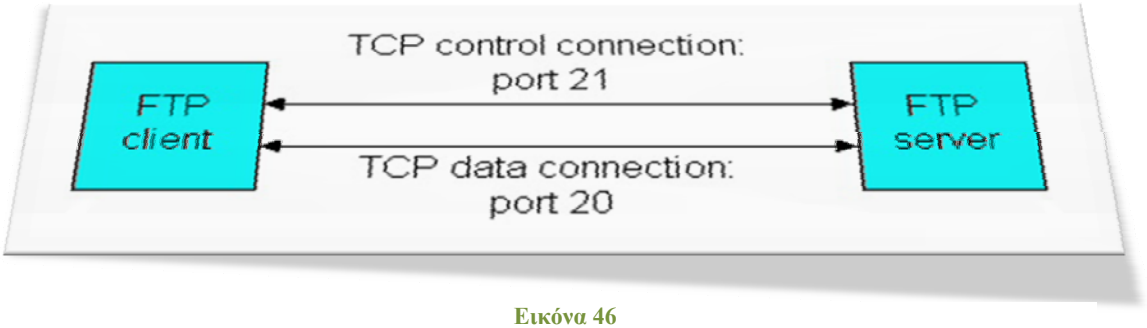


Εικόνα 45

Ο χρήστης πρώτα παρέχει το όνομα του απομακρυσμένου υπολογιστή (remote host name), με αποτέλεσμα η FTP διαδικασία πελάτη στον τοπικό υπολογιστή να εγκαθιστά μία σύνδεση TCP με τον εξυπηρετητή FTP στον απομακρυσμένο υπολογιστή. Τότε ο χρήστης παρέχει το user name και το password, τα οποία στέλνονται μέσω της σύνδεσης TCP ως μέρος εντολών FTP. Μετά την πιστοποίηση του χρήστη από τον εξυπηρετητή, ο χρήστης μπορεί να αντιγράψει ή να μετακινήσει ένα

ή περισσότερα αρχεία από το τοπικό του σύστημα αρχείων προς το απομακρυσμένο σύστημα αρχείων, και αντιστρόφως.

Το FTP χρησιμοποιεί δύο παράλληλες συνδέσεις TCP για την μεταφορά ενός αρχείου: μία **σύνδεση ελέγχου (control connection)** και μία **σύνδεση δεδομένων (data connection)**. Η σύνδεση ελέγχου χρησιμοποιείται για την μεταφορά πληροφοριών ελέγχου μεταξύ των δύο υπολογιστών, πληροφορίες όπως το όνομα χρήστη (user name), τον κωδικό, για την αλλαγή του απομακρυσμένου καταλόγου και εντολές για την ανάκτηση (get) ή καταχώρηση (put) αρχείων. Η σύνδεση δεδομένων χρησιμοποιείται για την πραγματική μεταφορά του αρχείου. Εξαιτίας της ύπαρξης δύο TCP συνδέσεων, λέμε ότι το FTP μεταφέρει την πληροφορία ελέγχου **εκτός ζώνης (out-of-band)**. Αντίθετα στα πρωτόκολλα που χρησιμοποιούν μόνο μία σύνδεση λέμε ότι η πληροφορία ελέγχου μεταφέρεται εντός ζώνης (in-band). Στο παρακάτω σχήμα φαίνονται οι δύο ξεχωριστές TCP συνδέσεις που χρησιμοποιεί το FTP.



Εικόνα 46

Όταν ο χρήστης ξεκινά μία FTP σύνοδο με κάποιον απομακρυσμένο υπολογιστή, το FTP πρώτα εγκαθιστά μία TCP σύνδεση ελέγχου στην θύρα (port) 21 του FTP εξυπηρετητή. Ο FTP πελάτης στέλνει το αναγνωριστικό και τον κωδικό του χρήστη μέσω της σύνδεσης ελέγχου. Επίσης, μέσω της σύνδεσης ελέγχου ο FTP πελάτης στέλνει και εντολές για την αλλαγή του απομακρυσμένου καταλόγου. Όταν ο χρήστης ζητήσει μία μεταφορά αρχείου (από η προς τον απομακρυσμένο υπολογιστή) το FTP ανοίγει μία TCP σύνδεση δεδομένων στην θύρα 20 του FTP εξυπηρετητή. Μέσω αυτής της σύνδεσης δεδομένων στέλνεται μόνο ένα αρχείο και στη συνέχεια η σύνδεση δεδομένων κλείνει. Αν κατά τη διάρκεια αυτής της συνόδου ο χρήστης θέλει να μεταφέρει και άλλα αρχεία τότε ανοίγονται ξεχωριστές συνδέσεις δεδομένων, μία για κάθε αρχείο. Επομένως, στο FTP η σύνδεση ελέγχου παραμένει για όλη τη διάρ-

κεια της συνόδου, ενώ χρησιμοποιείται μία ξεχωριστή σύνδεση δεδομένων για κάθε αρχείο που μεταφέρεται μεταξύ των δύο υπολογιστών.

Κατά την διάρκεια της συνόδου ο εξυπηρετητής κρατάει την κατάσταση (state) του χρήστη. Για κάθε σύνοδο έχουμε μία ξεχωριστή σύνδεση ελέγχου που συσχετίζεται με την λογαριασμό του χρήστη, και ο εξυπηρετητής κρατά το τρέχοντα κατάλογο του χρήστη στον λογαριασμό αυτό. Εξαιτίας της πληροφορίας για την κατάσταση των συνόδων των χρηστών έχουμε σημαντική μείωση στον αριθμό των χρηστών που μπορεί να εξυπηρετηθούν ταυτόχρονα, σε σχέση με άλλα πρωτόκολλα που δεν κρατάνε την κατάσταση του χρήστη, όπως το HTTP.

Τελειώνοντας την περιγραφή του FTP, θα αναφερθούμε στις εντολές (commands) και τις αποκρίσεις (replies) που χρησιμοποιεί. Οι εντολές από τον πελάτη προς τον εξυπηρετητή και οι αποκρίσεις από τον εξυπηρετητή προς τον πελάτη στέλνονται μέσω της TCP σύνδεσης ελέγχου σε 7-bit ASCII κωδικοποίηση, και είναι αναγνώσιμες. Για τον διαχωρισμό των εντολών μεταξύ τους χρησιμοποιείται αλλαγή γραμμής και κάθε εντολή αποτελείται από τέσσερις κεφαλαίους ASCII χαρακτήρες και από κάποια προαιρετικά ορίσματα. Μερικές από τις πιο συχνά χρησιμοποιούμενες εντολές φαίνονται στον παρακάτω πίνακα.

4.2.6 ICMP

Πρωτόκολλο ICMP : (Internet Control Message Protocol). Το ICMP είναι ένα από τα βασικά πρωτόκολλα του διαδικτύου. Χρησιμοποιείται κυρίως από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους, όπως για παράδειγμα την έλλειψη κάποιας υπηρεσίας από έναν server ή την απουσία ενός υπολογιστή από το δίκτυο.

Το πρωτόκολλο ICMP διαφέρει από τα πρωτόκολλα TCP και UDP διότι συνήθως δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του σύστημα. Εξαίρεση σε αυτό τον κανόνα αποτελεί το εργαλείο ping, το οποίο στέλνει μηνύματα ICMP Echo Request σε κάποιον υπολογιστή του δικτύου για να διαπιστώσει εάν ο υπολογιστής αυτός υπάρχει ή όχι και επίσης πόσο χρόνο χρειάζεται το μήνυμα να φτάσει σε αυτόν. Εάν ο υπολογιστής αυτός υπάρχει, θα απαντήσει με μηνύματα Echo Response.

Τεχνικές Λεπτομέρειες

Το πρωτόκολλο ICMP έχει τυποποιηθεί στα έγγραφα RFC 792 και RFC 1122. Η έκδοση του πρωτοκόλλου που χρησιμοποιείται πιο συχνά είναι η έκδοση 4, η οποία ονομάζεται και ICMPv4 και αποτελεί μέρος του IPv4. Το IPv6 διαθέτει ένα αντίστοιχο πρωτόκολλο το οποίο ονομάζεται ICMPv6.

Τα μηνύματα ICMP κατασκευάζονται στο επίπεδο δικτύου και αποτελούν κανονικά πακέτα IP. Όπως και το πρωτόκολλο UDP, το ICMP δεν εγγυάται ότι το πακέτο θα φτάσει αξιόπιστα στον προορισμό του. Μερικές από τις πιο συνηθισμένες δικτυακές εφαρμογές χρησιμοποιούν πακέτα ICMP, όπως για παράδειγμα η εντολή traceroute. Η εντολή αυτή χρησιμοποιείται για την εύρεση όλων των κόμβων ενός δικτύου από τους οποίους πρέπει να περάσει ένα πακέτο για να φτάσει στον τελικό προορισμό του. Αυτό που κάνει ουσιαστικά είναι να στέλνει πακέτα UDP με συγκεκριμένο χρόνο ζωής (TTL - Time To Live) και να περιμένει πακέτα ICMP που να περιέχουν μήνυμα σφάλματος "ο χρόνος ζωής τελείωσε" (Time To Live exceeded in transit) ή "ο προορισμός δεν βρέθηκε" (Destination unreachable). Στο σημείο αυτό αξίζει να αναφερθεί ότι ο χρόνος ζωής (TTL - Time To Live) ενός πακέτου είναι ο μέγιστος αριθμός των κόμβων του δικτύου από τους οποίους θα πρέπει να περάσει έως ότου φτάσει στον προορισμό του. Εάν ένα πακέτο κατά την πορεία του στο δίκτυο περάσει από περισσότερους κόμβους απ' ότι αναγράφεται στο πεδίο TTL, τότε το πακέτο αυτομάτως απορρίπτεται και ο υπολογιστής ο οποίος διαπίστωσε το σφάλμα στέλνει ένα ICMP μήνυμα σφάλματος στον υπολογιστή που δημιούργησε το πακέτο. Τέλος, η εντολή ping χρησιμοποιεί επίσης το πρωτόκολλο ICMP για την λειτουργία της και συγκεκριμένα τα ICMP μηνύματα "Echo request" και "Echo reply".

Λίστα μηνυμάτων ελέγχου ICMP

1 - Echo Reply	17 - Reserved for security
2 - Reserved	18-29 - Reserved for robustness experiment
3 - Destination Unreachable	30 - Traceroute
4 - Source Quench	31 - Datagram Conversion Error
5 - Redirect Message	32 - Mobile Host Redirect
6 - Alternate Host Address	33 - IPv6 Where-Are-You
7 - Reserved	34 - IPv6 Here-I-Am
8 - Router Advertisement	35 - Mobile Registration Request
9 - Router Solicitation	36 - Mobile Registration Reply
10 - Time Exceeded	37 - Domain Name Request
11 - Parameter Problem	38 - Domain Name Reply
12 - Timestamp	39 - SKIP Algorithm Discovery Protocol, Simple Key-Management for Internet Protocol
13 - Timestamp Reply	40 - Photuris, Security failures
14 - Information Request	41 - ICMP for experimental mobility protocols such as Seamoby [RFC4065]
15 - Address Mask Request	42-255 - Reserved
16 - Address Mask Reply	

Δομή πακέτου ICMP

Στο σχήμα που ακολουθεί φαίνεται η κεφαλίδα (header) ενός πακέτου ICMP. Με γκρι χρώμα απεικονίζεται η κεφαλίδα που προκύπτει από το πρωτόκολλο IP και με πράσινο χρώμα η κεφαλίδα που προκύπτει από το πρωτόκολλο ICMP. Ακολουθεί επεξήγηση των πεδίων της ICMP κεφαλίδας. Τα πεδία της IP κεφαλίδας εξηγούνται στο άρθρο για το IP-Internet Protocol.

+	Bits 0–3	4–7	8–15	16–18	19–31
0	Version	IHL	TOS/DSCP/ECN	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	IP Header Checksum	
96	Source Address				
128	Destination Address				
160	Type		Code	Checksum	
192	ID			Sequence	

Εικόνα 47

4.2.7 UDP

Πρωτόκολλο UDP : (User Datagram Protocol). Το πρωτόκολλο UDP είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Μία εναλλακτική ονομασία του πρωτοκόλλου είναι **Universal Datagram Protocol**. Διάφορα προγράμματα χρησιμοποιούν το πρωτόκολλο UDP για την αποστολή σύντομων μηνυμάτων (γνωστών και ως datagrams) από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών.

Ένα από τα κύρια χαρακτηριστικά του UDP είναι ότι δεν εγγυάται αξιόπιστη επικοινωνία. Τα πακέτα UDP που αποστέλλονται από έναν υπολογιστή μπορεί να φτάσουν στον παραλήπτη με λάθος σειρά, διπλά ή να μην φτάσουν καθόλου εάν το δίκτυο έχει μεγάλο φόρτο. Αντιθέτως, το πρωτόκολλο TCP διαθέτει όλους τους απαραίτητους μηχανισμούς ελέγχου και επιβολής της αξιοπιστίας και συνεπώς μπορεί να εγγυηθεί την αξιόπιστη επικοινωνία μεταξύ των υπολογιστών. Η έλλειψη των μηχανισμών αυτών από το πρωτόκολλο UDP το καθιστά αρκετά πιο γρήγορο και αποτελεσματικό, τουλάχιστον για τις εφαρμογές εκείνες που δεν απαιτούν αξιόπιστη επικοινωνία.

Οι εφαρμογές audio και video streaming χρησιμοποιούν κατά κόρον πακέτα UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα ούτως ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Κατά συνέπεια προτιμάται το πρωτόκολλο UDP διότι είναι αρκετά γρήγορο, παρόλο που υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ούτως ώστε ο τελικός χρήστης να μην παρατηρεί καμία αλλοίωση ή διακοπή στην ροή του ήχου και της εικόνας λόγω του χαμένου πακέτου. Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Η τελευταία δυνατότητα χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές.

Μερικές σημαντικές εφαρμογές που χρησιμοποιούν πακέτα UDP είναι οι εξής: Domain Name System (DNS), IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) και τα παιχνίδια που παίζονται ζωντανά μέσω του Διαδικτύου.

Δομή UDP πακέτου

Η δομή ενός πακέτου UDP περιγράφεται αναλυτικά στο αντίστοιχο πρότυπο IETF [RFC 768]. Στην σουίτα πρωτοκόλλων του Διαδικτύου, το UDP βρίσκεται ανάμεσα στο επίπεδο δικτύου (network layer) και στο επίπεδο συνόδου (session layer) ή εφαρμογών (application layer).

Κάθε πακέτο UDP έχει μία κεφαλίδα (header) που αναφέρει τα χαρακτηριστικά του. Η κεφαλίδα περιλαμβάνει μονάχα 4 πεδία, τα οποία είναι πολύ λίγα εάν συγκριθούν με άλλα πρωτόκολλα, όπως το TCP. Δύο από τα τέσσερα πεδία είναι προαιρετικά (φαίνονται χρωματισμένα με ροζ).

+	Bits 0 - 15	16 - 31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

Εικόνα 48

Ακολουθεί μία συνοπτική εξήγηση των πεδίων:

Source port

Η πόρτα του αποστολέα από την οποία προήλθε το πακέτο. Εάν ο παραλήπτης επιθυμεί να στείλει κάποια απάντηση, θα πρέπει να την στείλει στην πόρτα αυτήν. Το συγκεκριμένο πεδίο δεν είναι υποχρεωτικό και στις περιπτώσεις που δεν χρησιμοποιείται θα πρέπει να έχει την τιμή μηδέν.

Destination port

Η πόρτα του παραλήπτη στην οποία θα πρέπει να παραδοθεί το πακέτο.

Length

Το πεδίο αυτό έχει μέγεθος 16-bit και περιλαμβάνει το μέγεθος του πακέτου σε bytes. Το μικρότερο δυνατό μέγεθος είναι 8 bytes, αφού η κεφαλίδα αυτή καθ' αυτή καταλαμβάνει τόσο χώρο. Θεωρητικά, το μέγεθος του UDP πακέτου δεν μπορεί να ξεπερνάει τα 65,527 bytes, αλλά πρακτικά το όριο μειώνεται στα 65,507 bytes λόγω διαφόρων περιορισμών που εισάγει το πρωτόκολλο IPv4 στο επίπεδο δικτύου.

Checksum

Ένα πεδίο 16-bit το οποίο χρησιμοποιείται για επαλήθευση της ορθότητας του πακέτου στο σύνολό του, δηλαδή τόσο της κεφαλίδας όσο και των δεδομένων.

Στην συνέχεια το πακέτο UDP περνάει στο επίπεδο δικτύου, το οποίο αναλαμβάνει να το μεταδώσει στο δίκτυο υπολογιστών. Το επίπεδο αυτό τοποθετεί μία ακόμη κεφαλίδα στο πακέτο, η οποία διαφέρει ανάλογα με την έκδοση του πρωτοκόλλου που χρησιμοποιείται στο επίπεδο δικτύου (IPv4 ή IPv6).

- Για **IPv4**, το πακέτο λαμβάνει την ακόλουθη μορφή:

+	Bits 0 - 7	8 - 15	16 - 23	24 - 31
0	Source address			
32	Destination address			
64	Zeros	Protocol	UDP length	
96	Source Port		Destination Port	
128	Length		Checksum	
160	Data			

Εικόνα 49

Source Address, Destination Address

Οι διευθύνσεις IP του αποστολέα και του παραλήπτη αντίστοιχα.

Zeros

Μία ακολουθία μηδενικών, η οποία δεν παίζει κανέναν ρόλο κατά την μετάδοση του πακέτου.

Protocol

Ένας χαρακτηριστικός αριθμός που αντιστοιχεί στο πρωτόκολλο που χρησιμοποιείται. Για το UDP η τιμή που παίρνει το πεδίο αυτό είναι 17.

UDP Lenght

Το συνολικό μέγεθος του πακέτου UDP.

- Για **IPv6**, το πακέτο παίρνει την εξής μορφή:

<table>
<tr><th>+</th><th>Bits 0 - 7</th><th>8 - 15</th><th>16 - 23</th><th>24 - 31</th></tr>
<tr><td>0</td><td colspan="4" rowspan="4">Source address</td></tr>
<tr><td>32</td></tr>
<tr><td>64</td></tr>
<tr><td>96</td></tr>
<tr><td>128</td><td colspan="4" rowspan="4">Destination address</td></tr>
<tr><td>160</td></tr>
<tr><td>192</td></tr>
<tr><td>256</td></tr>
<tr><td>288</td><td colspan="4">UDP length</td></tr>
<tr><td>320</td><td colspan="3">Zeros</td><td>Next Header</td></tr>
<tr><td>352</td><td colspan="2">Source Port</td><td colspan="2">Destination Port</td></tr>
<tr><td>384</td><td colspan="2">Length</td><td colspan="2">Checksum</td></tr>
<tr><td>416</td><td colspan="4">Data</td></tr>
</table>

Εικόνα 50

Source Address, Destination Address

Οι διευθύνσεις IP του αποστολέα και του παραλήπτη αντίστοιχα, οι οποίες όμως στην περίπτωση αυτή είναι τύπου IPv6, δηλαδή πολύ μεγαλύτερες (IPv4 - 32bit, IPv6 - 128bit).

UDP Lenght

Το συνολικό μέγεθος του πακέτου UDP, όπως και προηγουμένως.

Zeros

Μία ακολουθία μηδενικών, η οποία δεν παίζει κανέναν ρόλο κατά την μετάδοση του πακέτου.

Next Header

Το πεδίο αυτό παίρνει μία τιμή που είναι χαρακτηριστική για το πρωτόκολλο που χρησιμοποιείται. Στην περίπτωση του UDP, η τιμή αυτή είναι 17.

Τέλος, αξίζει να σημειωθεί ότι στην περίπτωση IPv6 το πεδίο checksum του UDP πακέτου δεν είναι πλέον προαιρετικό, αλλά θα πρέπει υποχρεωτικά να συμπληρωθεί.

Εφαρμογές

Όπως αναφέρθηκε και προηγουμένως, οι εφαρμογές που χρησιμοποιούν το πρωτόκολλο UDP θα πρέπει να μπορούν να δεχτούν κάποια απώλεια πακέτων ή διάφορα σφάλματα στα πακέτα τα οποία στέλνουν. Μερικές εφαρμογές, όπως για παράδειγμα το Trivial File Transfer Protocol (TFTP) υλοποιούν δικούς τους μηχανισμούς διασφάλισης της αξιοπιστίας της επικοινωνίας. Πάντως, τις περισσότερες φορές οι εφαρμογές που χρησιμοποιούν το UDP δεν επιβάλλουν επιπρόσθετους μηχανισμούς αξιοπιστίας διότι θα παρεμποδίζονται από αυτούς και χειροτερεύει η απόδοσή τους. Κλασικό παράδειγμα τέτοιων προγραμμάτων είναι οι εφαρμογές πραγματικού χρόνου (πχ. media streaming, παιχνίδια στο διαδίκτυο, VoIP κτλ). Στην περίπτωση πάντως που μία εφαρμογή χρειάζεται αξιόπιστη μετάδοση δεδομένων, δηλαδή η πλειοψηφία των εφαρμογών του διαδικτύου, θα προτιμήσει να χρησιμοποιήσει το πρωτόκολλο TCP αντί του UDP.

Σε ένα τυπικό δίκτυο υπολογιστών, η κίνηση που προέρχεται από την μετάδοση UDP πακέτων ανέρχεται σε ένα αρκετά μικρό ποσοστό. Παρόλα αυτά όμως, το

πρωτόκολλο αυτό το χρησιμοποιούν πολύ σημαντικές εφαρμογές, στην σωστή λειτουργία των οποίων βασίζεται το διαδίκτυο. Τέτοιες εφαρμογές είναι για παράδειγμα οι εξής: Domain Name System (DNS), Simple Network Management Protocol (SNMP), Dynamic Host Configuration Protocol (DHCP) και το Routing Information Protocol (RIP)

4.2.8 NETBIOS

Πρωτόκολλο NETBIOS : (Network Basic Input / Output System).Το NETBIOS είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται από τα windows για name resolution. Δεν χρησιμοποιεί κάποιο συγκεκριμένο configuration αλλά ένα σετ παραμέτρων που καθορίζει τον τρόπο επικοινωνίας των μηχανημάτων. Υπάρχουν τέσσερις βασικοί παράμετροι αυτοί είναι:

- Τύπος (0x01) Ο πελάτης θα χρησιμοποιήσει UDP broadcasts για επικοινωνία.
- Τύπος (0x02) Ο πελάτης θα χρησιμοποιήσει UDP unicasts προς ένα Wins εξυπηρετητή.
- Τύπος (0x04) Ο πελάτης θα χρησιμοποιήσει πρώτα broadcasts 0x01 και μετά unicast UDP πακέτα επικοινωνίας (0x02).
- Τύπος (0x08) Ο πελάτης θα χρησιμοποιήσει πρώτα unicast και μετά broadcast UDP πακέτα.

Ο καθορισμένος τύπος που χρησιμοποιείται στα Windows είναι ο 0x01. Η χρήση δε του Netbios που είναι η πιο αποτελεσματική είναι η 0x08. Τα NETBIOS ονόματα δε δεν μπορούν να ξεπερνούν τους 16 χαρακτήρες. Κατά τη διαδικασία της εκκίνησης σε κάθε NETBIOS δίκτυο ξεκινάει η διαδικασία εκλογής για τη δημιουργία ενός Domain Master Browser (DMB).

Ο DMB στη συνέχεια έρχεται σε επικοινωνία με όλους τους LMB (Local Master Browsers) που βρίσκει και εξάγει από αυτούς browse list περιεχόμενα. Κάθε 11 με 15 λεπτά μια νέα εκλογή για DMB θα καθορίσει ποιος θα είναι ο νέος DMB για το συγκεκριμένο DOMAIN με κριτήρια το uptime, protocol version και os level.

Το NetBIOS παρέχει τη σύνοδο και τις υπηρεσίες μεταφορών που περιγράφονται στο Ανοικτών Συστημάτων του μοντέλου **(OSI).** Ωστόσο, δεν παρέχει ένα

σταθερό πλαίσιο ή τη μορφή των δεδομένων για τη διαβίβαση. Ένα τυπικό πλαίσιο μορφής παρέχεται από NetBUI (NetBIOS Extended User Interface).

4.2.9 SMTP (Simple Mail Transfer Protocol)

Πρωτόκολλο SMTP : (Simple Mail Transfer Protocol). Το SMTP είναι το πρωτόκολλο του στρώματος εφαρμογών που χρησιμοποιείται για την μεταφορά των μηνυμάτων του ηλεκτρονικού ταχυδρομείου. Το SMTP χρησιμοποιεί ως πρωτόκολλο του στρώματος μεταφοράς το TCP και συγκεκριμένα τη θύρα 25 και βασικά έχει δύο τμήματα: την πλευρά του πελάτη (client side), που είναι ο εξυπηρετητής ταχυδρομείου του αποστολέα και την πλευρά του εξυπηρετητή (server side), που είναι ο εξυπηρετητής ταχυδρομείου του παραλήπτη. Ο κάθε εξυπηρετητής ταχυδρομείου μπορεί να παίξει το ρόλο είτε του πελάτη είτε του εξυπηρετητή: όταν αποστέλλει ένα μήνυμα έχει το ρόλο του πελάτη, ενώ όταν δέχεται μηνύματα έχει το ρόλο του εξυπηρετητή.

Το SMTP είναι ένα πρωτόκολλο χαρακτήρων ASCII των 7-bit. Ο λόγος αυτής της επιλογής βρίσκεται πίσω στο 1982 όταν εκδόθηκε το πρωτόκολλο SMTP. Την εποχή εκείνη τα μηνύματα του ηλεκτρονικού ταχυδρομείου αποτελούνταν μόνο από απλό κείμενο και η επιλογή της κωδικοποίησης των χαρακτήρων με 7-bit ήταν λογική. Στις μέρες μας όμως τα μηνύματα του ηλεκτρονικού ταχυδρομείου δεν περιλαμβάνουν μόνο απλό κείμενο αλλά και εικόνες, ήχους κτλ. τα οποία κωδικοποιούνται με 8-bit. Επομένως, για την μεταφορά τους χρειάζεται πρώτα η μετατροπή τους στα 7-bit, η αποστολή στον παραλήπτη σε μορφή 7-bit και η μετατροπή τους από τον παραλήπτη πίσω στην μορφή των 8 bit.

Θα εξετάσουμε το πρωτόκολλο SMTP με ένα παράδειγμα τυπικής αποστολής ενός μηνύματος ηλεκτρονικού ταχυδρομείου. Έστω ότι ο Α στέλνει ένα e-mail στον Β. Τότε ακολουθείτε η ακόλουθη διαδικασία:

- Ο Α ξεκινάει το πρόγραμμα για την αποστολή e-mail, που στην ουσία είναι ένας αντιπρόσωπος χρήστη, στο οποίο παρέχει τη διεύθυνση e-mail του Β και με το οποίο συνθέτει το μήνυμα. Τέλος, ο Α δίνει την εντολή για αποστολή του μηνύματος.

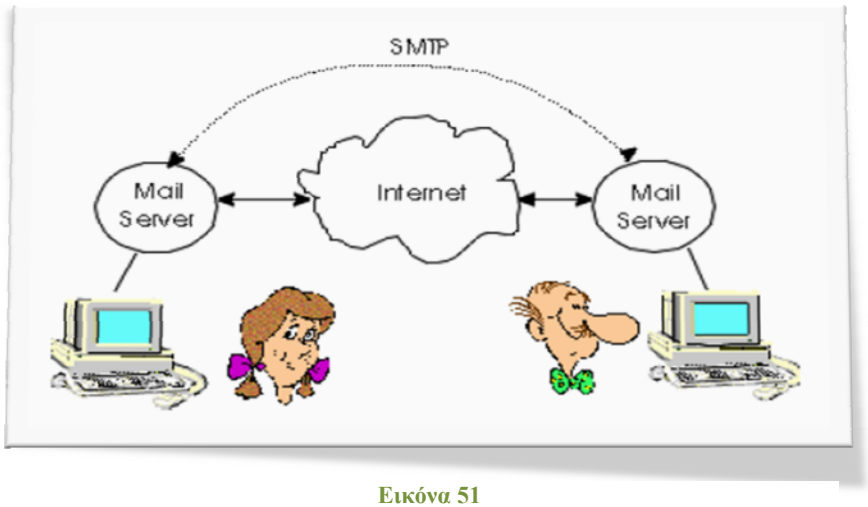
- Ο αντιπρόσωπος χρήστη του Α στέλνει το μήνυμα στον αντιπρόσωπος ταχυδρομείου της, όπου μπαίνει σε στην εξερχόμενη ουρά αποστολής.

- Ο αντιπρόσωπος ταχυδρομείου του Α βλέπει το μήνυμα στην ουρά και ενεργώντας ως πελάτης ανοίγει μία TCP σύνδεση με τον πράκτορα ταχυδρομείου του Β στη θύρα 25, μέσω της οποίας στέλνονται τα SMTP μηνύματα.

- Μετά από κάποιου είδους χειραψίας (handshake), η οποία θα περιγραφεί αναλυτικά παρακάτω, στέλνεται το μήνυμα στον αντιπρόσωπο ταχυδρομείου του Β.

- Η πλευρά εξυπηρετητή του εξυπηρετητή ταχυδρομείου του Β λαμβάνει το μήνυμα και το τοποθετεί στο mailbox του Β.

- Ο Β χρησιμοποιώντας τον αντιπρόσωπο χρήστη διαβάζει το μήνυμα.



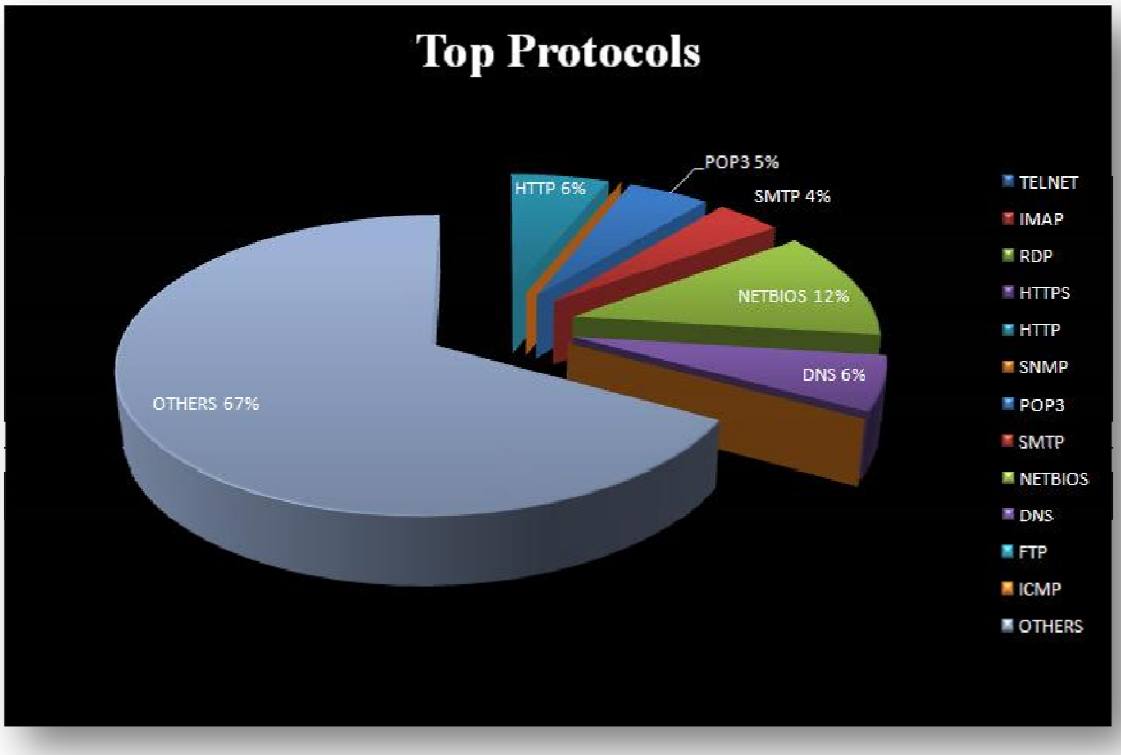
Εικόνα 51

Μία σημαντική παρατήρηση: το μήνυμα δεν αποθηκεύεται σε κάποιον ενδιάμεσο εξυπηρετητή ταχυδρομείου του Διαδικτύου και για την αποστολή του μέσω του SMTP ανοίγεται μία απευθείας σύνδεση μεταξύ του εξυπηρετητή ταχυδρομείου του αποστολέα και του εξυπηρετητή ταχυδρομείου του παραλήπτη.

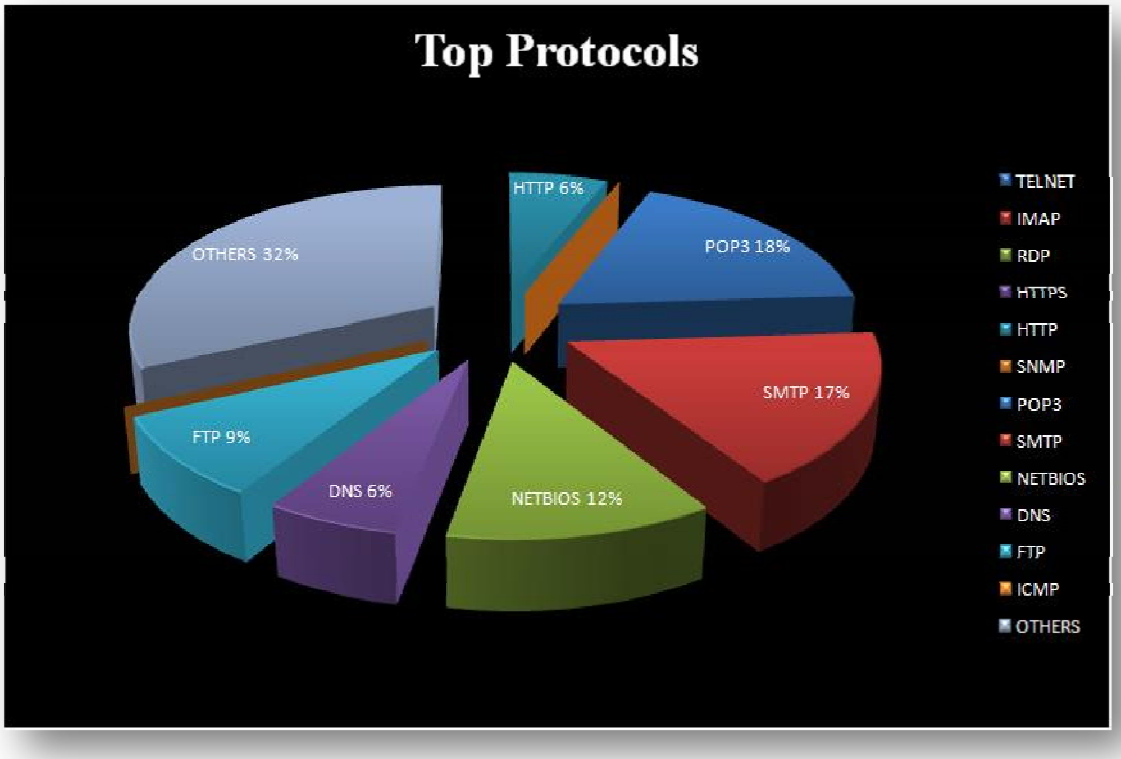
Ας δούμε αναλυτικά τη λειτουργία του SMTP. Στην αρχή ανοίγεται μία TCP σύνδεση στη θύρα 25 μεταξύ των εξυπηρετητών ταχυδρομείου του αποστολέα και

του παραλήπτη. Στη συνέχεια πραγματοποιείτε μία μορφή χειραψίας: Στην αρχή οι δύο εξυπηρετητές ταχυδρομείου γνωστοποιούν ο ένας στον άλλον τη διεύθυνσή τους. Στη συνέχεια η πλευρά του πελάτη του εξυπηρετητή ταχυδρομείου του αποστολέα γνωστοποιεί στην πλευρά εξυπηρετητή του εξυπηρετητή ταχυδρομείου του παραλήπτη τις e-mail διευθύνσεις του αποστολέα και του παραλήπτη. Στη συνέχεια στέλνεται το ίδιο το μήνυμα. Αν ο πελάτης έχει και να στείλει και άλλα μηνύματα προς τον ίδιο εξυπηρερτητή ταχυδρομείου τότε τα στέλνει μέσω της ίδιας TCP σύνδεσης. Μετά την αποστολή και του τελευταίου μηνύματος η πλευρά του πελάτη τερματίζει την σύνδεση TCP.

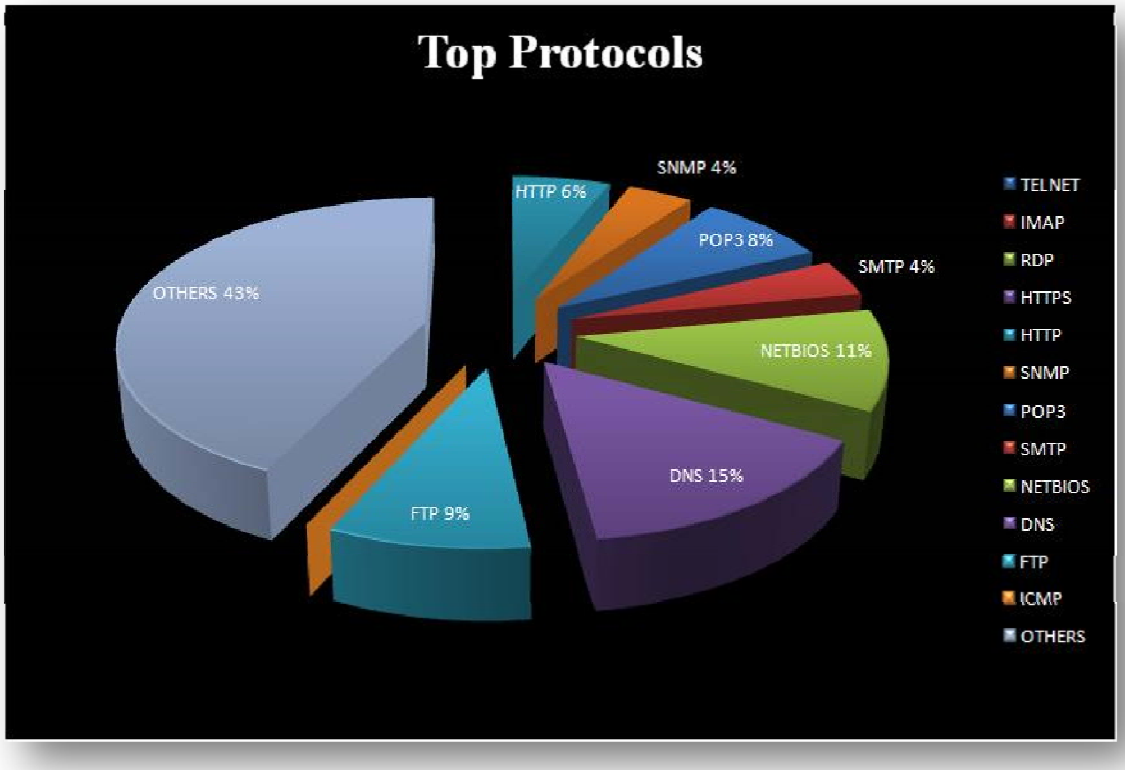
4.2.11 Διαγράμματα Μετρήσεων Top Protocols



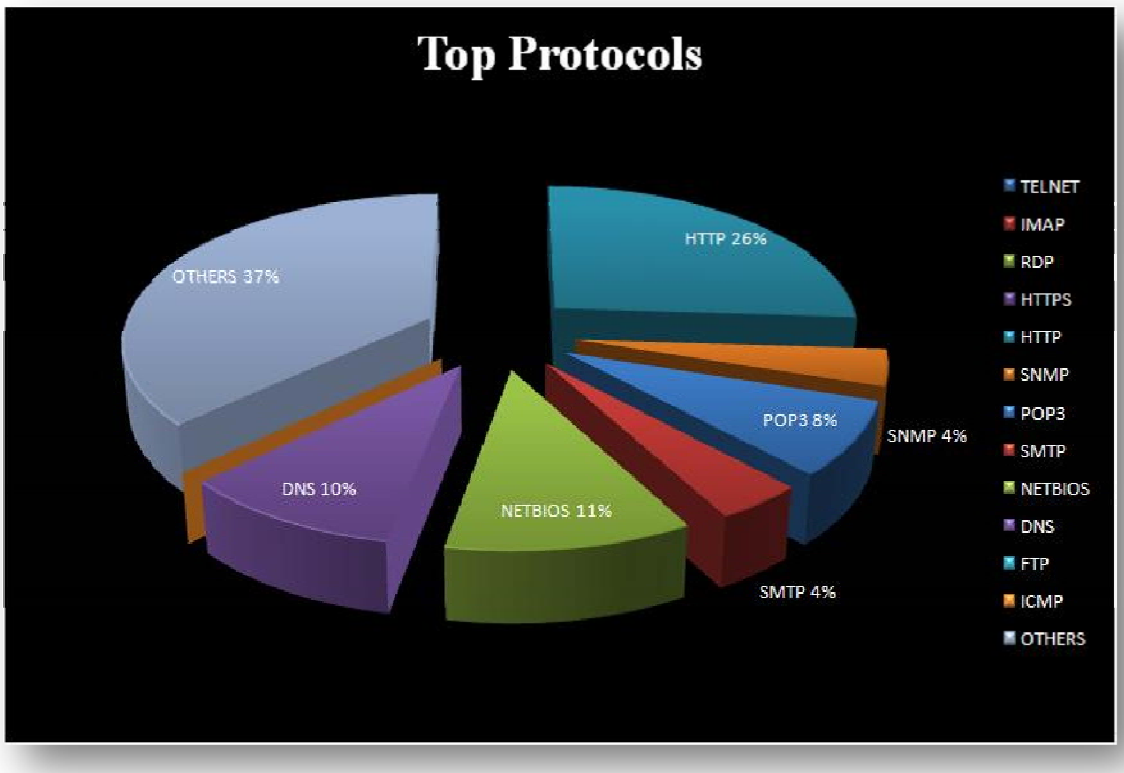
Εικόνα 52



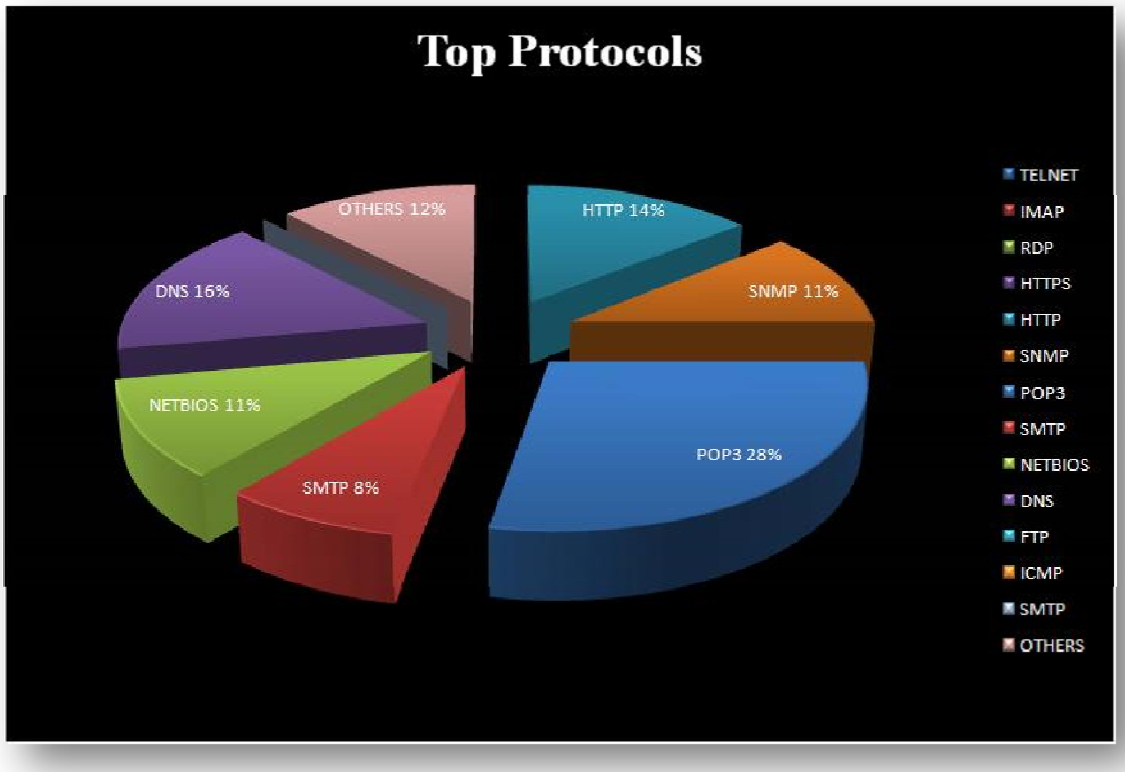
Εικόνα 53



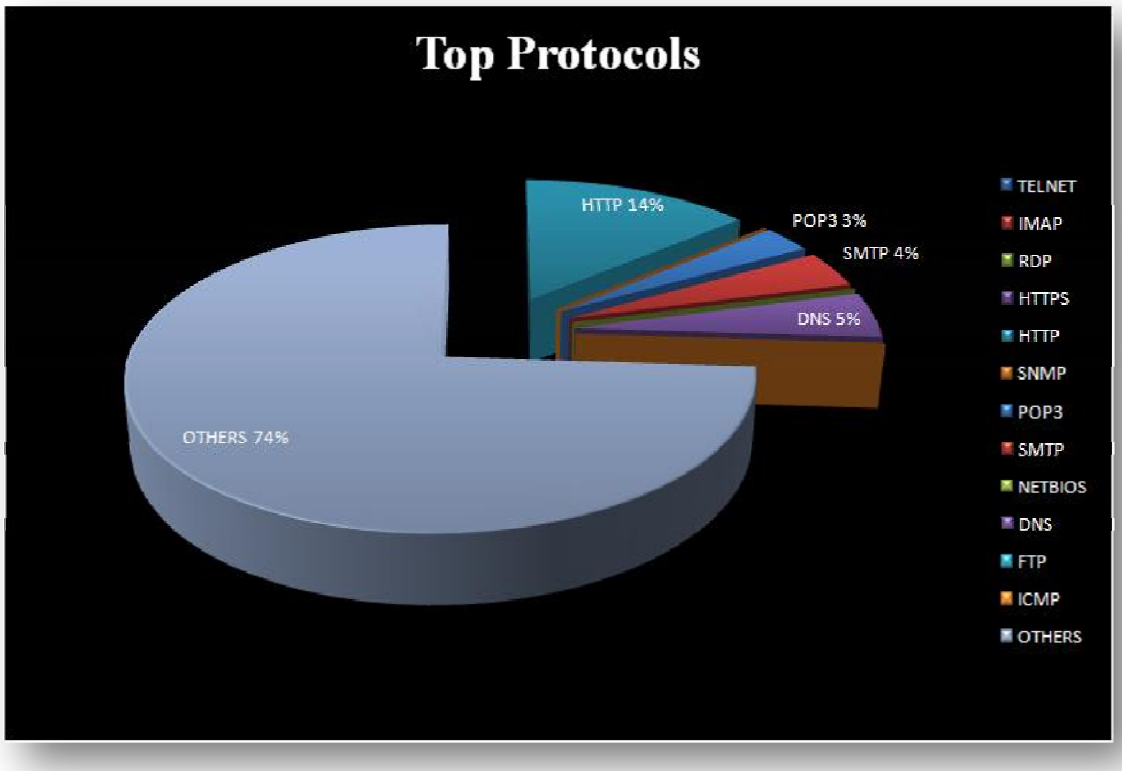
Εικόνα 54



Εικόνα 55

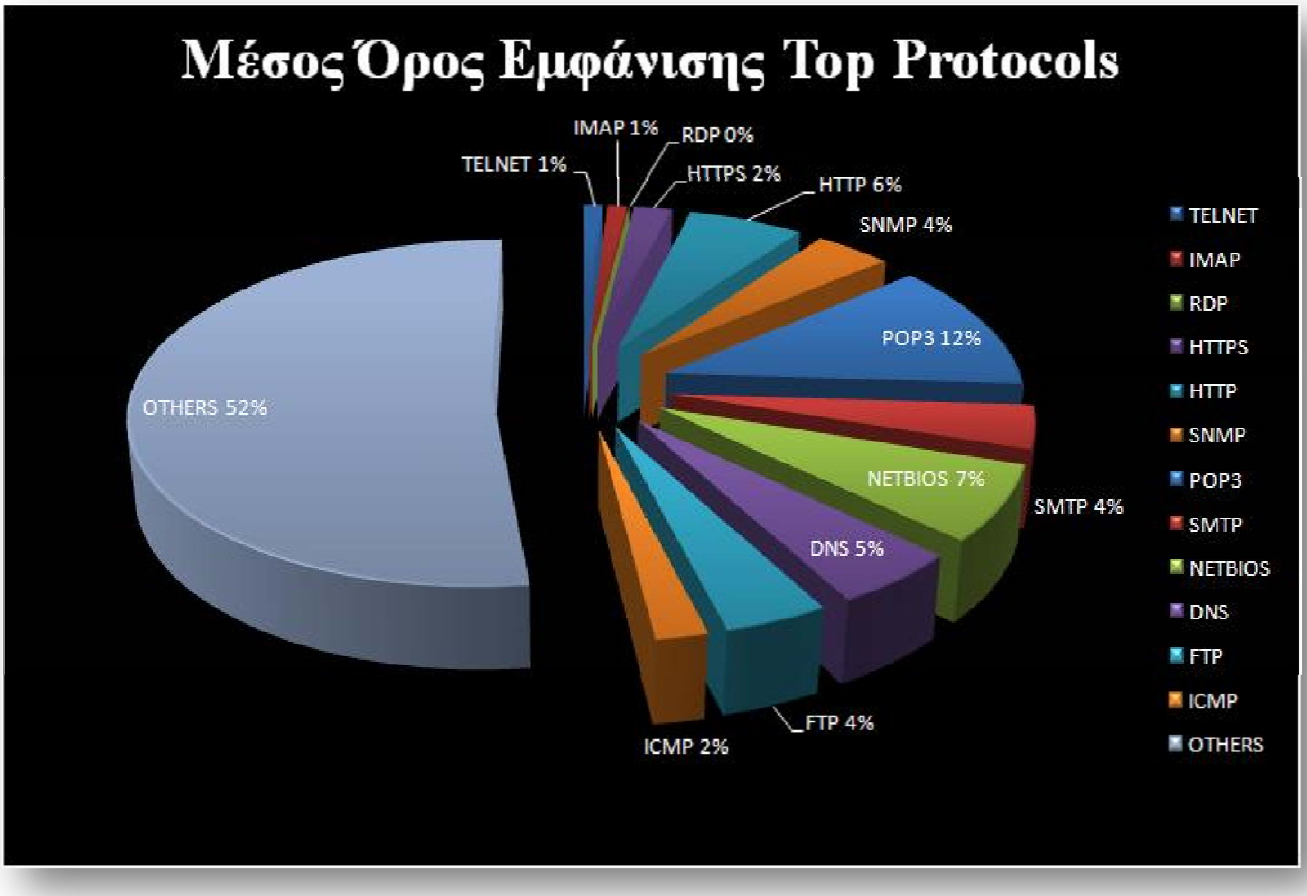


Εικόνα 56



Εικόνα 57

4.2.12 Διάγραμμα Μέσου Όρου Top Protocols

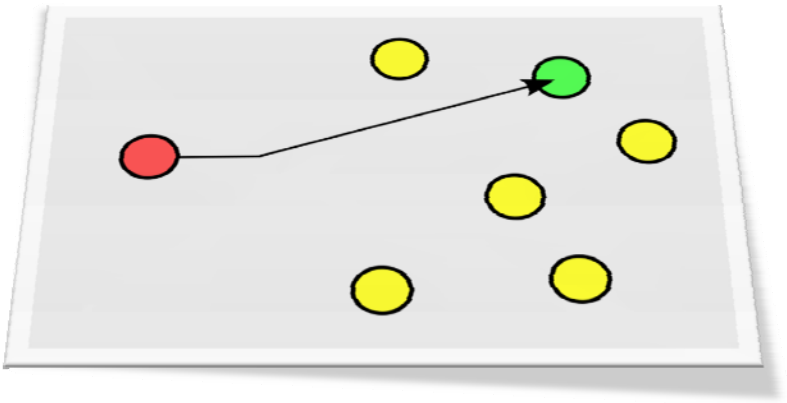


Εικόνα 58

4.5 Unicast Packets

Σ' ένα δίκτυο υπολογιστών, η τεχνική μετάδοσης unicast είναι η αποστολή μηνυμάτων με προορισμό έναν και μόνο κεντρικό υπολογιστή μέσα από ένα πακέτο δικτυακών μεταγωγών. Η λογική του Unicast σχηματίζεται σε αναλογία με αυτήν του broadcast ,η οποία βασίζεται στη μετάδοση των ίδιων δεδομένων προς όλους τους δυνατούς προορισμούς. Μια άλλη τεχνική μετάδοσης σε πολλούς προορισμούς είναι η multicast, η οποία αποστέλλει δεδομένα μόνο στους ενδιαφερόμενους δέκτες χρησιμοποιώντας ειδικές εντολές διευθύνσεων.

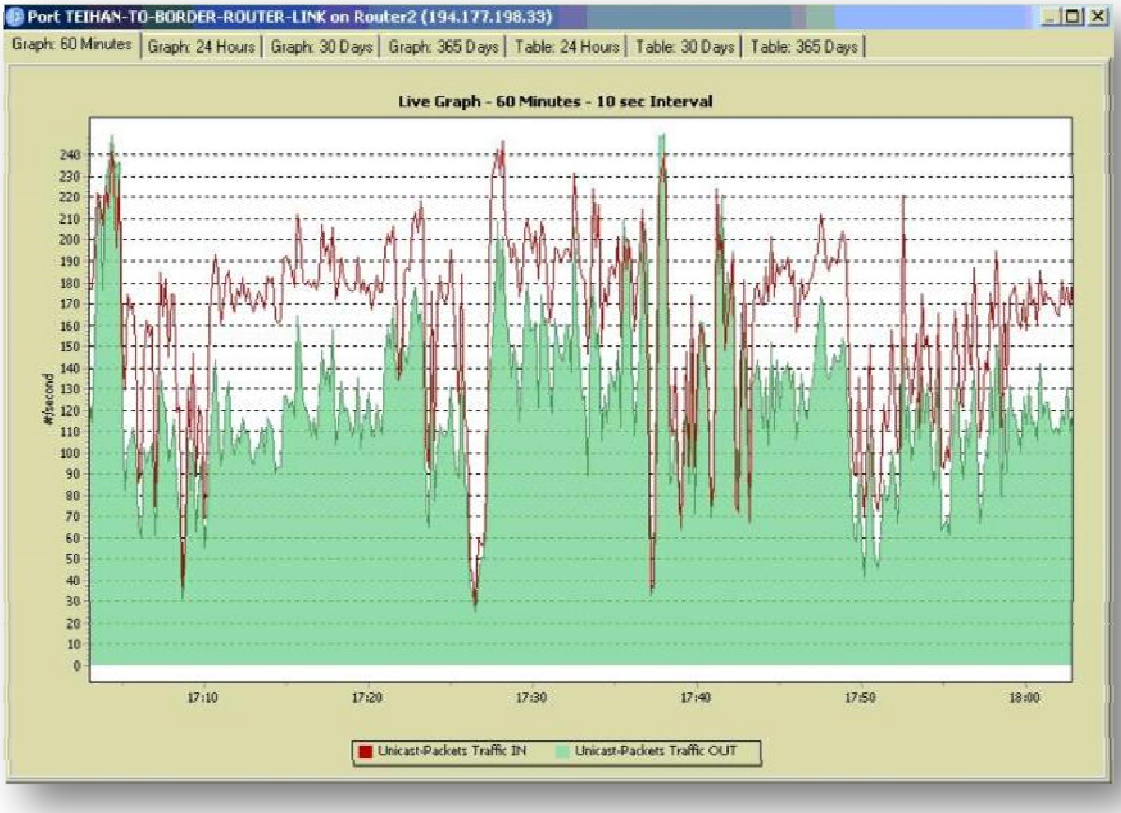
Η τεχνική μετάδοσης unicast χρησιμοποιείται για κάθε δικτυακή επεξεργασία στην οποία απαιτείται μια μοναδική ή ιδιωτική πηγή. Οι δικτυακές εφαρμογές, οι οποίες κατανέμουν πολλά πακέτα είναι ιδιαίτερα δαπανηρές στη διεξαγωγή τους με την τεχνική unicast, κι αυτό γιατί κάθε σύνδεση δικτύου καταναλώνει υπολογιστικούς πόρους του κεντρικού υπολογιστή που εκτελεί την αποστολή και απαιτεί το δικό του ξεχωριστό bandwidth για την μετάδοση των πληροφοριών. Τέτοιου είδους εφαρμογές συμπεριλαμβάνουν τη ροή οπτικοακουστικών μέσων πολλών τυπων, π.χ. .wav , .avi , .mp3 , .mpeg κ.α. Ένα παράδειγμα αυτής της εφαρμογής είναι η μετάδοση ραδιοφώνου μέσω internet η οποία γίνεται με χρήση της τεχνικής μεθόδου unicast καταναλώνοντας ένα μεγάλο κομμάτι του bandwidth.

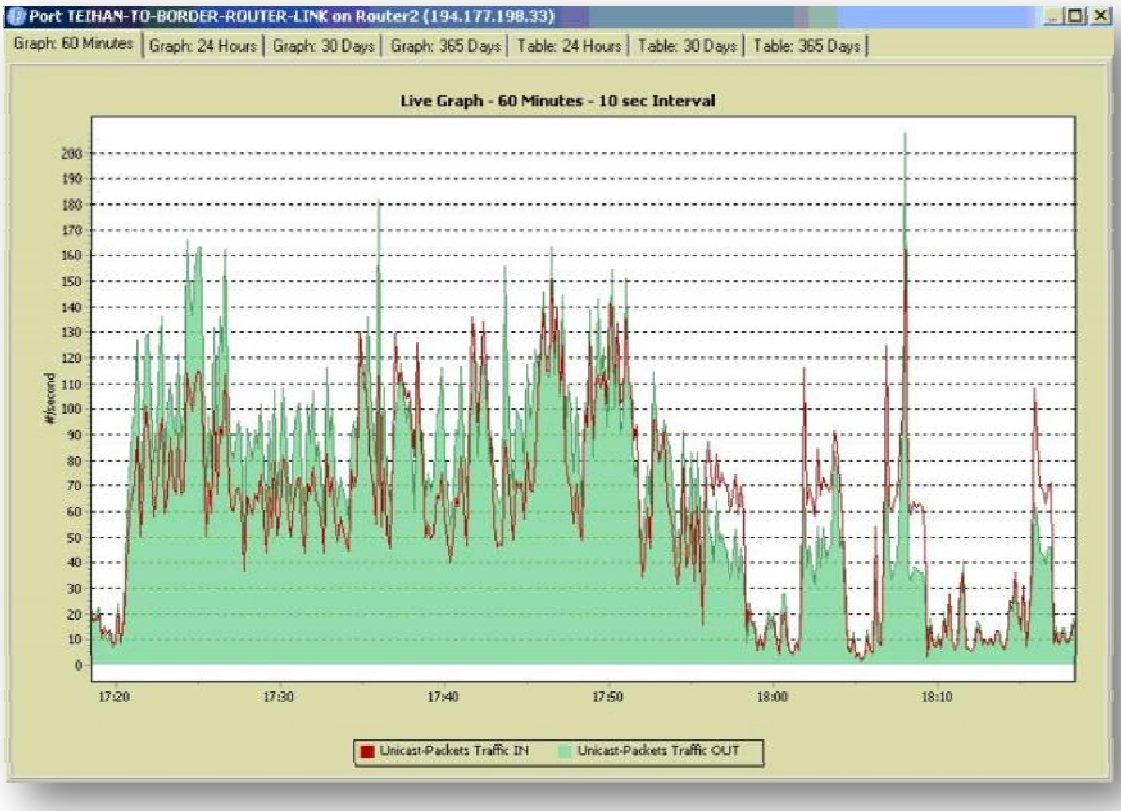


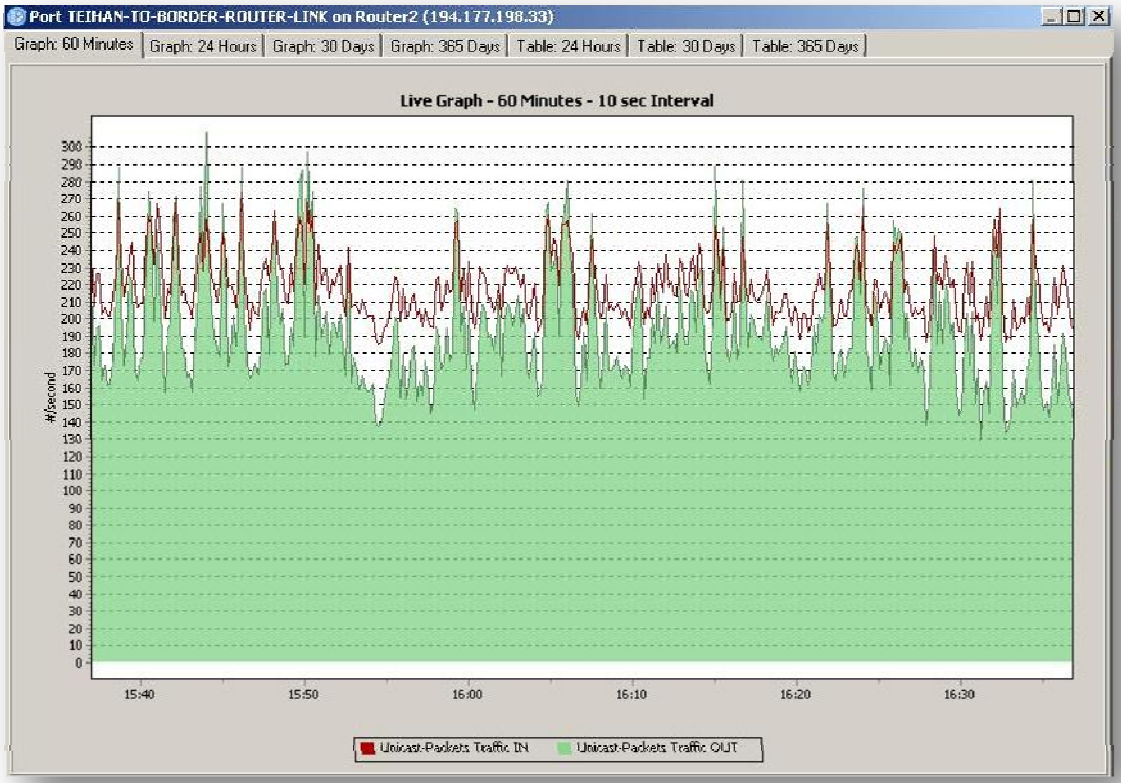
Εικόνα 59.Τεχνική μετάδοσης UNICAST

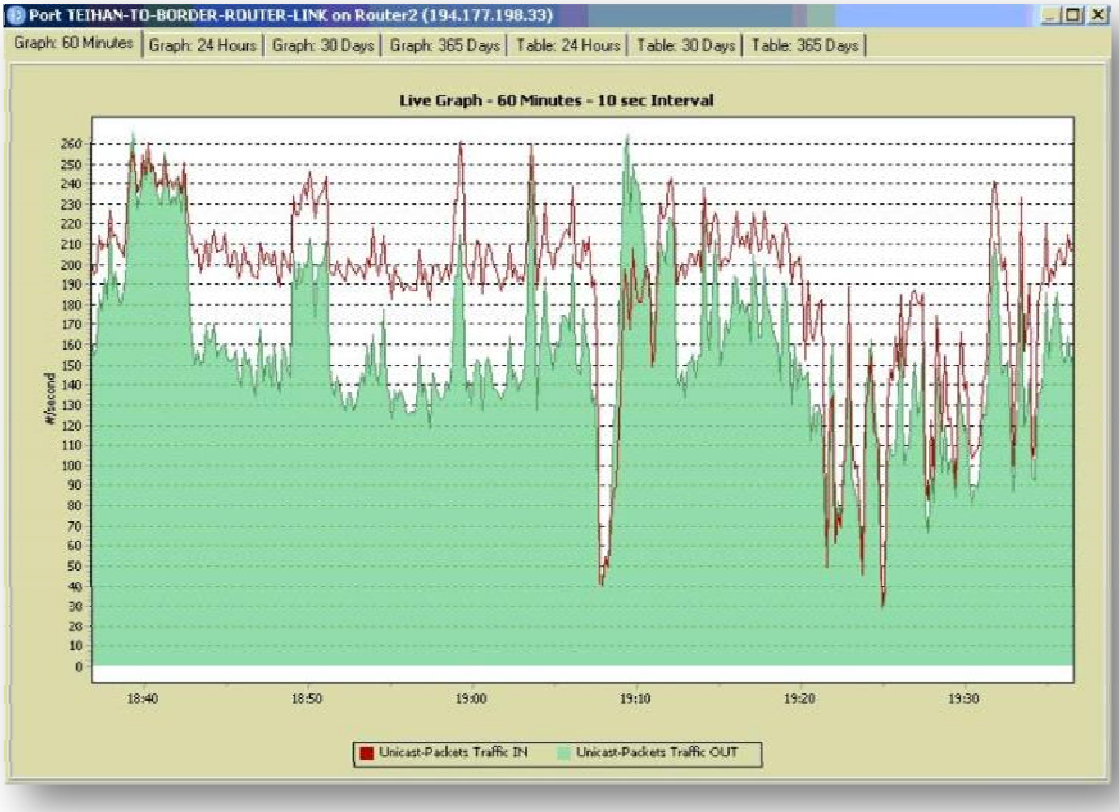
4.5.1 Μετρήσεις Unicast Packets (Γραφική Απεικόνιση)

4.5.1.1 Ωριαίες μετρήσεις

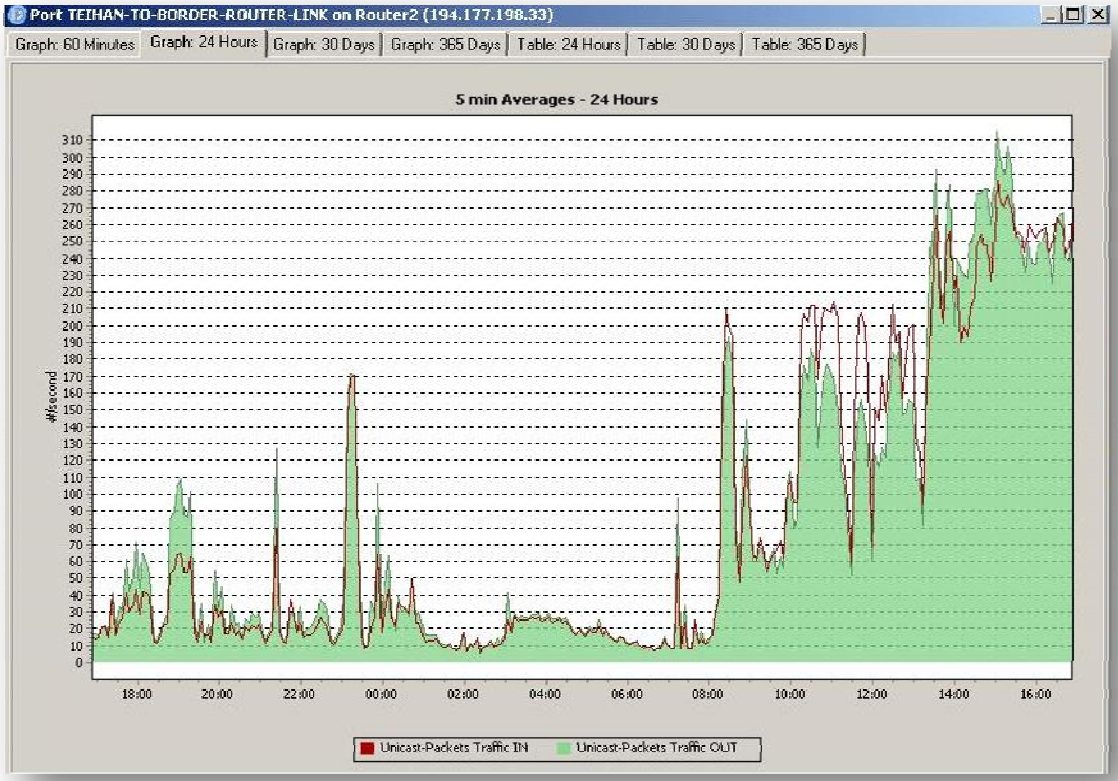


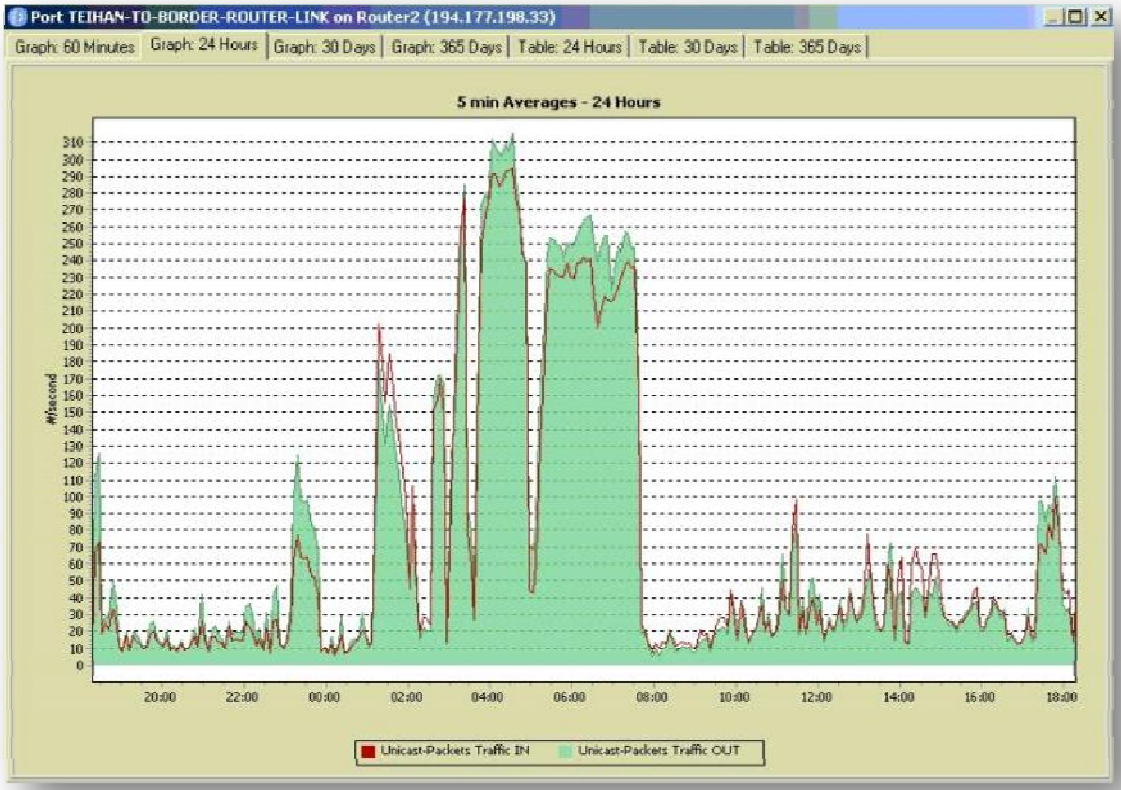


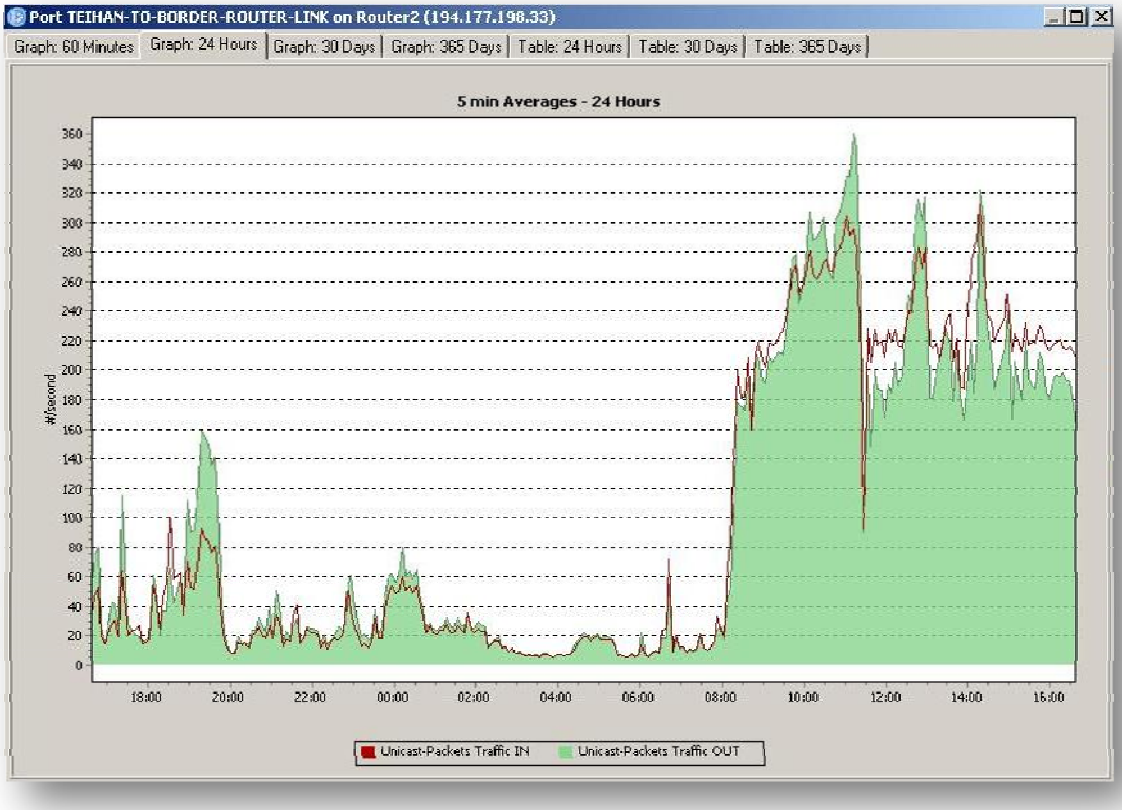

Port TEIHAN-TO-BORDER-ROUTER-LINK on Router2 (194.177.198.33)
Graph: 60 Minutes
Graph: 24 Hours
Graph: 30 Days
Graph: 365 Days
Table: 24 Hours
Table: 30 Days
Table: 365 Days
Live Graph - 60 Minutes - 10 sec Interval
#/Second
15:40
15:50
16:00
16:10
16:20
16:30
Unicast-Packets Traffic IN
Unicast-Packets Traffic OUT

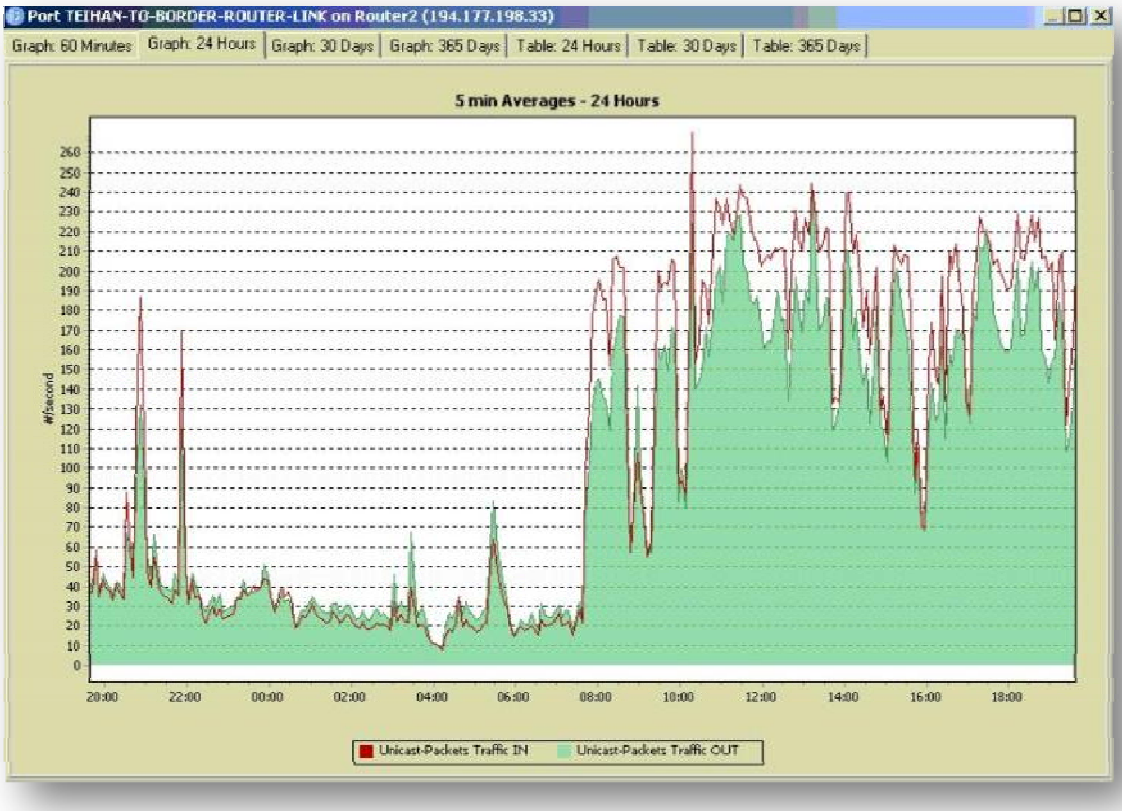

Port TEIHAN-TO-BORDER-ROUTER-LINK on Router2 (194.177.198.33)
Graph: 60 Minutes
Graph: 24 Hours
Graph: 30 Days
Graph: 365 Days
Table: 24 Hours
Table: 30 Days
Table: 365 Days
Live Graph - 60 Minutes - 10 sec Interval
#/second
18:40
18:50
19:00
19:10
19:20
19:30
Unicast-Packets Traffic IN
Unicast-Packets Traffic OUT

4.5.1.2 Ημερήσιες μετρήσεις

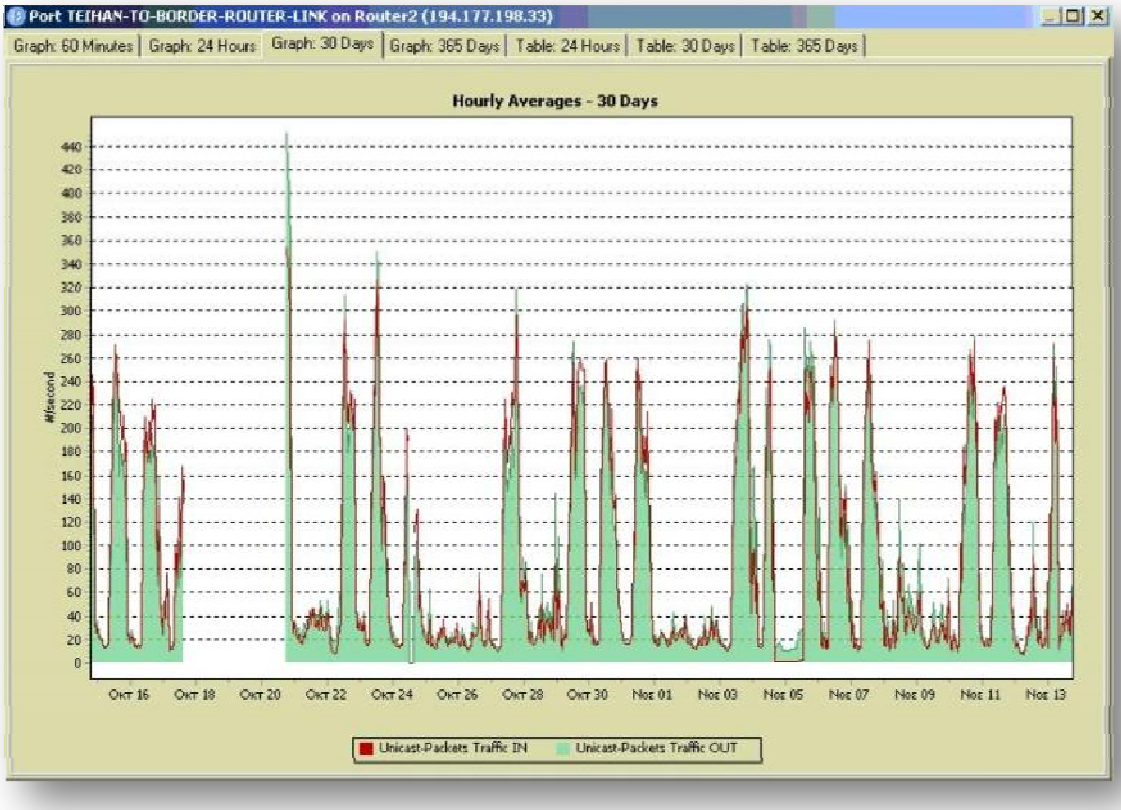


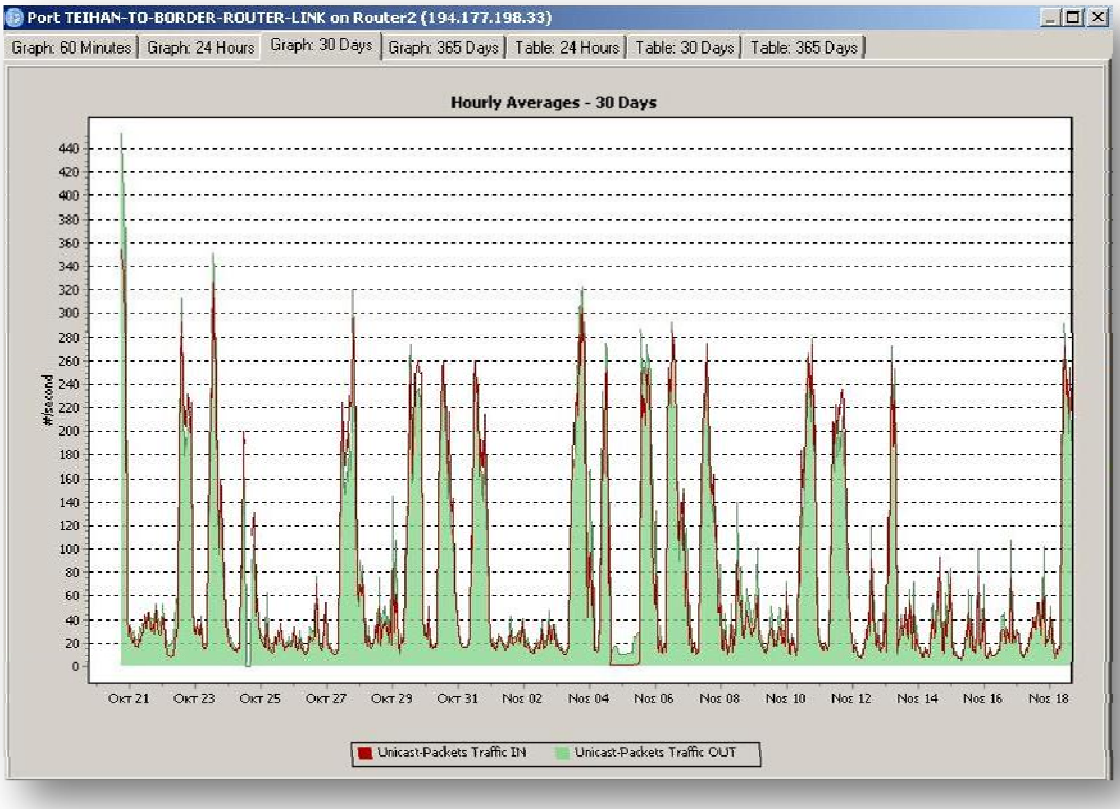



Port TEIHAN-TO-BORDER-ROUTER-LINK on Router2 (194.177.198.33)
Graph: 60 Minutes
Graph: 24 Hours
Graph: 30 Days
Graph: 365 Days
Table: 24 Hours
Table: 30 Days
Table: 365 Days
5 min Averages - 24 Hours
#/second
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
Unicast-Packets Traffic IN
Unicast-Packets Traffic OUT


Port TEIHAN-TO-BORDER-ROUTER-LINK on Router2 (194.177.198.33)
Graph: 60 Minutes
Graph: 24 Hours
Graph: 30 Days
Graph: 365 Days
Table: 24 Hours
Table: 30 Days
Table: 365 Days
5 min Averages - 24 Hours
#/second
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
Unicast-Packets Traffic IN
Unicast-Packets Traffic OUT

4.5.1.3 Μηνιαίες μετρήσεις





ΚΕΦΑΛΑΙΟ 5ο

5.1 Wireless TEI of Chania

Ως ασύρματο δίκτυο χαρακτηρίζεται το τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου. Σε παλαιότερες εποχές τα τηλεφωνικά δίκτυα ήταν αναλογικά, αλλά σήμερα όλα τα ασύρματα δίκτυα βασίζονται σε ψηφιακή τεχνολογία και, επομένως, κατά μία έννοια, είναι ουσιαστικώς δίκτυα υπολογιστών.

Στα ασύρματα δίκτυα εντάσσονται τα δίκτυα κινητής τηλεφωνίας, οι δορυφορικές επικοινωνίες, τα ασύρματα δίκτυα ευρείας περιοχής (WWAN), τα ασύρματα μητροπολιτικά δίκτυα (WMAN), τα ασύρματα τοπικά δίκτυα (WLAN) και τα ασύρματα προσωπικά δίκτυα (WPAN).

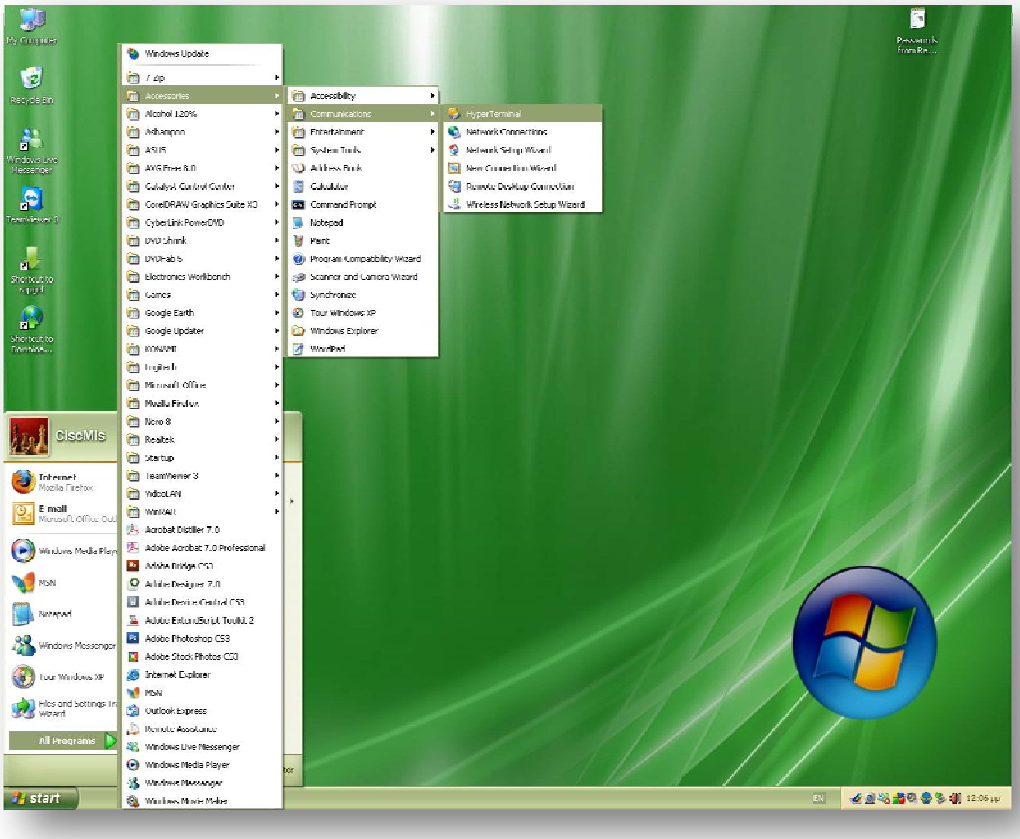
Η εγκατάσταση του ασύρματου δικτύου της σχολής πραγματοποιήθηκε με σκοπό την εξυπηρέτηση των σπουδαστών, προκειμένου να αποκτήσουν πρόσβαση στο Internet μέσω του Τεχνολογικού Εκπαιδευτικού Ιδρύματος. Με τη δημιουργία της ασύρματης δικτύωσης θα δημιουργηθούν περισσότερες θέσεις εργασίας και κατά συνέπεια θα αυξηθεί η ζήτηση του Bandwidth, κάτι το οποίο θα παρουσιάσει την ήδη υπάρχουσα αδυναμία των ταχυτήτων. Για την πραγματοποίηση μιας σωστής λειτουργίας και μιας αξιοπρεπούς διαχείρισης του ασύρματου δικτύου πραγματοποιήθηκαν τα Access Points βάση των δυνατοτήτων τους ώστε το σήμα τους να καλύπτει ένα μεγάλο κομμάτι του Ιδρύματος και η ακτινοβολία τους να μην ξεπερνά τα επιτρεπτά db που προβλέπονται σε δημόσιους χώρους. Στη συνέχεια του κεφαλαίου θα παρουσιαστεί το manual που επιμεληθήκαμε σύμφωνα με την παραμετροποίηση των Access Points Cisco Ap1300 καθώς και ο τρόπος διαχείρισης αυτών.

5.2 Manual Configuration

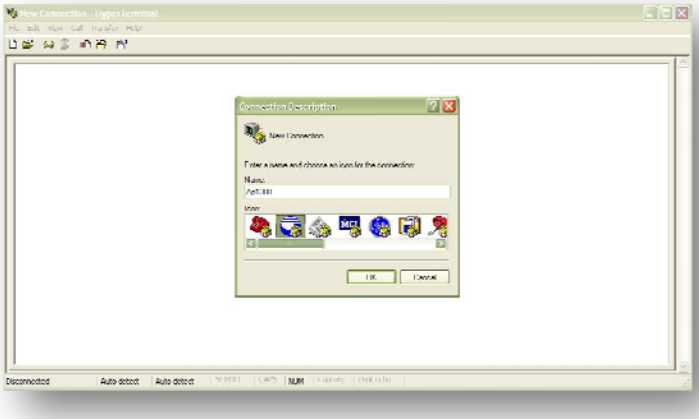
5.2.1 Λήψη κονσόλας Access Point Ap1300Cisco

Για τη λήψη κονσόλας του Access Point χρειαζόμαστε σειριακή θύρα στον υπολογιστή με τον οποίο θέλουμε να επικοινωνήσει το Access Point, ή μετατροπέα USB to serial στην περίπτωση που δεν μας παρέχει σειριακή ο υπολογιστής. Ενώνουμε λοιπόν με το καλώδιο που μας έχει προμηθεύσει η Cisco τα δύο μηχανήματα. Προσοχή, να συνδεθεί στην σωστή θύρα υποδοχής για κονσόλα του Access Point , διαφορετικά μπορεί να κάψουμε το interface της Ethernet.

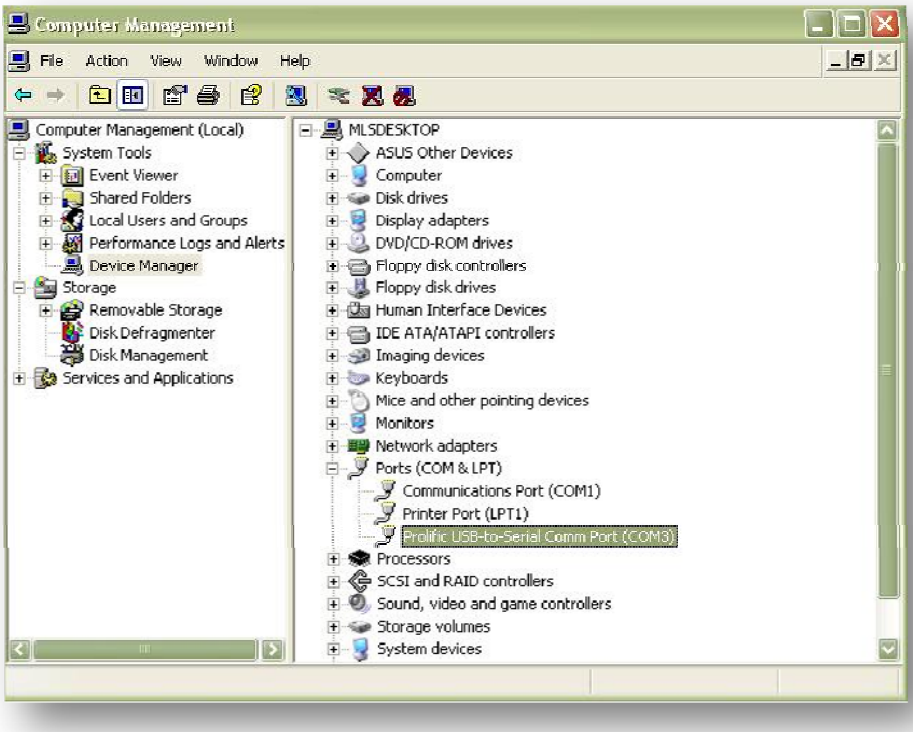
Στη συνέχεια ανοίγουμε το Hyper Terminal μέσα από τα Windows το οποίο θα βρούμε στο προορισμό Start → All Programs → Accessories → Communications → Hyper Terminal.

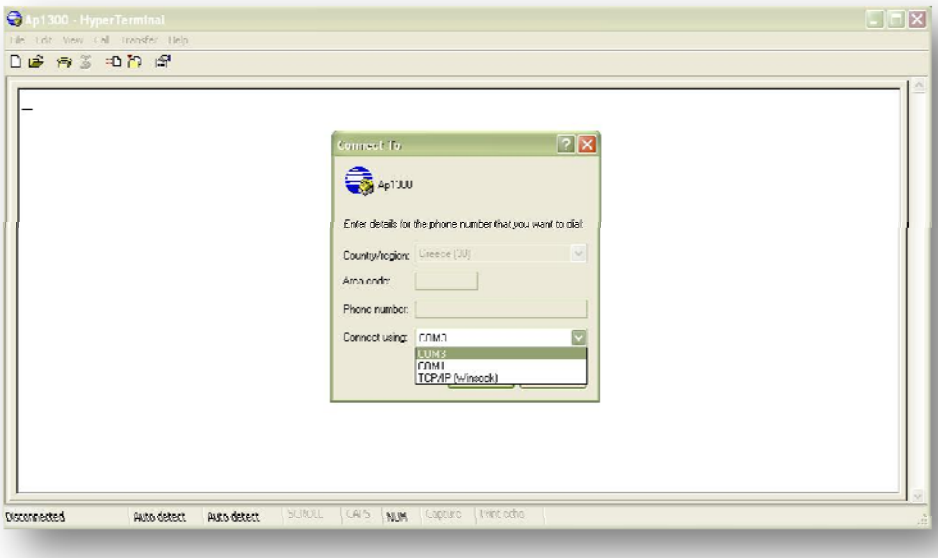


Κατά την εκκίνησή της η εφαρμογή μας ζητάει να σουμε μια νέα σύνδεση. Γραφούμε το όνομα της σύνδεσης , επιλέγουμε εικονίδιο και πατάμε OK , όπως βλέπουμε στην εικόνα.

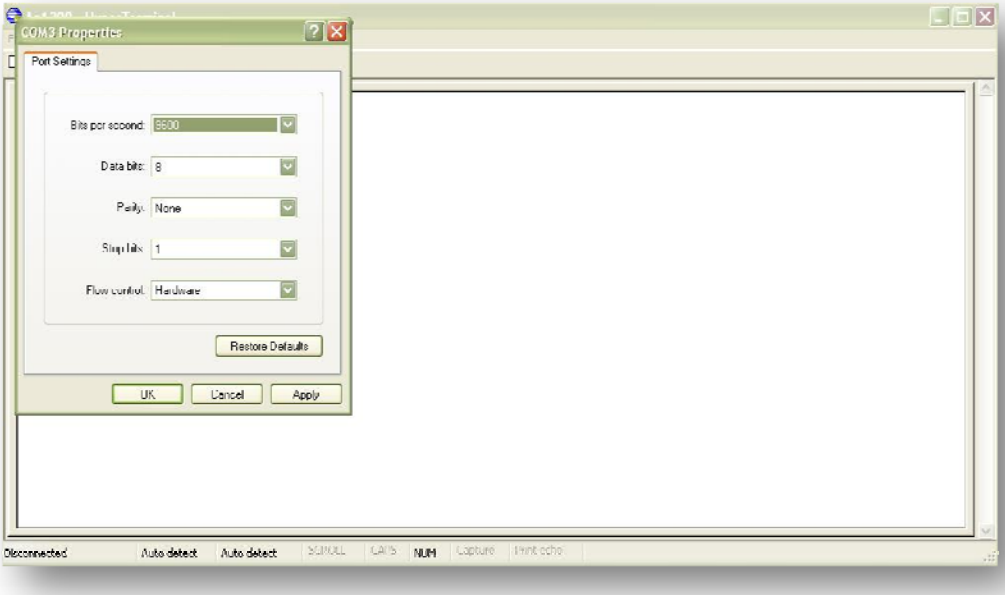


Στο παράθυρο Connect to που θα ανοίξει επιλέγουμε την θύρα επικοινωνίας COM στην οποία έχει συνδεθεί το καλώδιο της κονσόλας στον υπολογιστή μας. Αν η σειριακή βρίσκεται πάνω στο motherboard τότε ο αριθμός της θύρας είναι πάντα ο ίδιος και αρκεί να τον δούμε μια φορά μέσα από την διαχείριση συσκευών των Windows, αν κάνουμε χρήση κάποιου μετατροπέα USB to Serial κάθε φορά που τον συνδέουμε στον υπολογιστή ο αριθμός αυτός αλλάζει και πρέπει να τον ελέγχουμε.(εικ.3,4)



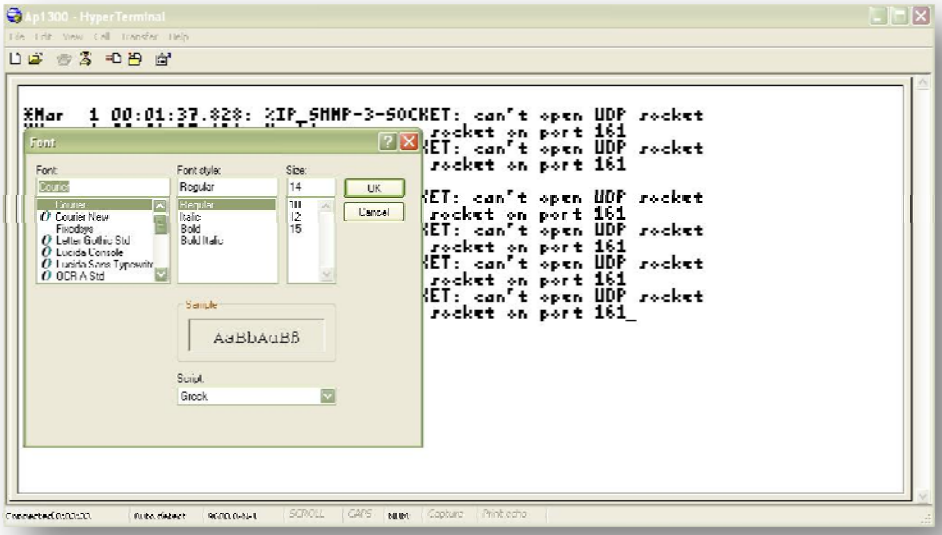


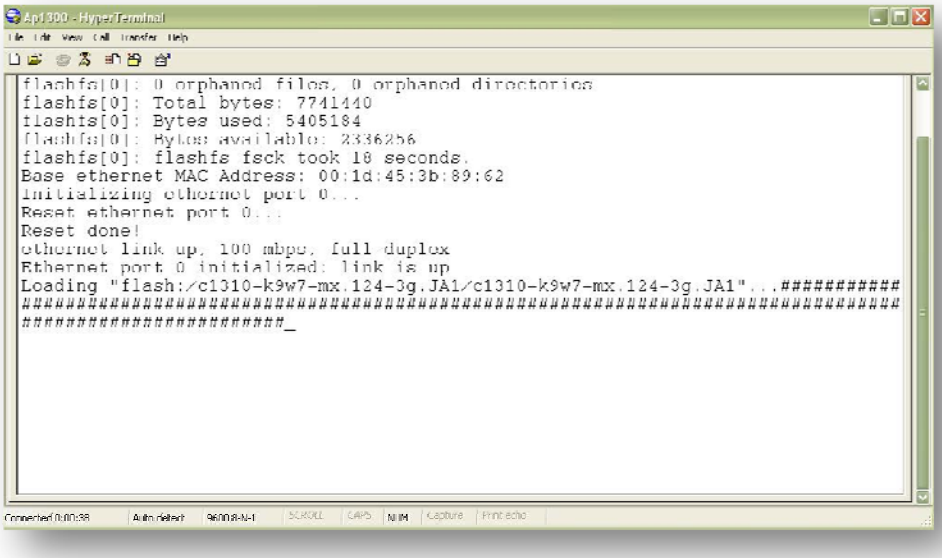
Στο παράθυρο COMx Properties εισάγουμε τις ρυθμίσεις για τη σωστή μετάδοση των δεδομένων της σειριακής επικοινωνίας. Bits per seconds : 9600, Data bits : 8, Parity : None ,Stop Bits : 1, Flow Control : Hardware και πατάμε OK. (εικ.5)



Αφού γίνει η σύνδεση θα εμφανιστεί κάτω δεξιά στο παράθυρο η επιγραφή Connected και ένα χρονόμετρο που μας δείχνει τη διάρκεια σύνδεσης. Δίνουμε ρεύμα στο Access Point και ξεκινάει η διδικασία φόρτωσης. Η προεπιλεγμένη γραμματοσει-

ρά του Hyper Terminal είναι η Terminal όπου μας εμποδίζει να διαβάσουμε το κείμενο φόρτωσης. Πηγαίνουμε στην επιλογή View → Fonts και επιλέγουμε την γραμματοσειρά Courier για να είναι πιο ευανάγνωστο το κείμενο.(εικ.6,7)





Μόλις φορτώσει το Access Point πατάμε Enter και δίνουμε τα παρακάτω στοιχεία για να μπορούμε να επέμβουμε με εντολές στην παραμετροποίηση του.

User Access Verification

Username: **xxxxx**

Password: **xxxxxxxxxxxxxx**

Noc_Ap_Chania_0X>

Αν κατά την διάρκεια που πληκτρολογούμε κάτι, εμφανιστούν κάποια μηνύματα όπως για παράδειγμα :

*Mar 1 00:04:37.813: %IP_SNMP-3-SOCKET: can't open UDP socket

*Mar 1 00:04:37.813: Unable to open socket on port 161

Είναι μηνύματα λειτουργίας του Access Point.Δεν δίνουμε σημασία και συνεχίζουμε κανονικά να πληκτρολογούμε.

5.2.2 Τοποθέτηση IP Address στο interface BVI 1

Για να πάρουμε το Access Point σε Web Browser θα πρέπει να του τοποθετήσουμε μια IP address στο interface BVI 1 μέσω κονσόλας. Η διαδικασία αυτή έχει ως εξής πληκτρολογώντας :

Noc_Ap_Chania_0X>**enable**

Noc_Ap_Chania_0X#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Noc_Ap_Chania_0X(config)#**interface bvi1**

Noc_Ap_Chania_0X(config-if)#**ip address 192.168.0.4 255.255.255.0**

Noc_Ap_Chania_0X(config-if)#**exit**

Noc_Ap_Chania_0X(config)#**exit**

Noc_Ap_Chania_0X#**write memory**

Building configuration...

[OK]

5.2.3 Έλεγχος IP Address στο interface BVI1

Για να ελέγξουμε αν η IP address που ορίσαμε εχει περαστεί στο interface BVI ,αφού είμαστε σε enable mode (Noc_Ap_Chania_0X>enable) πληκτρολογούμε τα εξής :

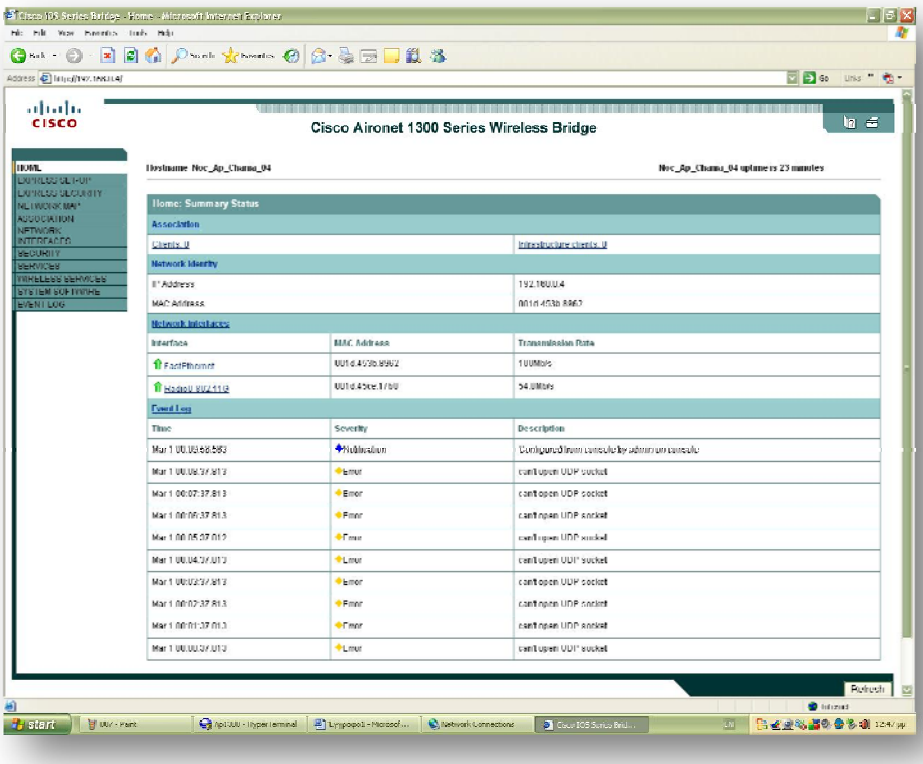
Noc_Ap_Chania_04# **show ip interface brief**

Interface	IP-Address	OK? Method Status	Protocol
BVI1	192.168.0.4	YES manual up	up
Dot11Radio0	unassigned	YES NVRAM up	up
FastEthernet0	unassigned	YES NVRAM up	up

Για να ολοκληρώσουμε την διαδικασία και να πάρουμε το Access Point από Web Browser θα πρέπει να αλλάξουμε την IP address του υπολογιστή μας ή η IP address που θα δώσουμε στο Access Point να είναι αντίστοιχη του τοπικού δικτύου που θα δημιουργήσουμε συνδέοντας με ένα straight UTP καλώδιο την Ethernet θήρα του Access Point με την κάρτα δικτύου του υπολογιστή μας. Αφού λοιπόν γίνουν όλα σωστά ανοίγουμε τον Internet Explorer (Προσοχή όχι Mozila FireFox 3 γιατί παρουσιάζονται προβλήματα λειτουργίας της σελίδας) και γράφουμε στην ad-

dress bar την IP address του Access Point που έχουμε δώσει.

Δίνουμε τα στοιχεία εισόδου που έχουμε ορίσει (user name : admin , password : NocAp1300Chania) ή αν δεν έχουν αλλαχθεί τα default στοιχεία όπου είναι : user name : Cisco , Password : Cisco και μας φέρνει σε Web Browser περιβάλλον το Access Point για πιο εύκολη παραμετροποίηση και χρήση του.



Παρακάτω επισημαίνονται κάποιες από τις βασικές ρυθμίσεις ,σε Web interface,που πραγματοποιήθηκαν στο Access Point για την ορθή λειτουργία του βα-ση των αναγκών της σχολή.

Network Interfaces: Radio0-802.11G Settings

Enable Radio: Enable

Role in Radio Network: Access Point

Data Rates: Best throughput

CCK Transmitter Power (mW): Max

OFDM Transmitter Power (mW): Max

Client Power (mW): Max

DefaultRadio Channel: Channel 9 – 2452 MHz

World Mode
Multi-Domain Operation: Disable

Radio Preamble Enable

Aironet Extensions: Enable

Ethernet Encapsulation Transform: 802.1H

Concatenation: Enable

Max Length of Concatenation: 3500

Reliable Multicast to WGB: Disable

Public Secure Packet Forwarding: Enable

Short Slot-Time: Enable

Beacon Privacy Guest-Mode: Enable

Clear Channel Assessment: Enable

Noise Floor Level: 50

Beacon Period: 100

Max. Data Retries: 64

Fragmentation Threshold: 4000

Data Beacon Rate (DTIM): 2

RTS Max. Retries: 64

RTS Threshold: 4000

Root Parent Timeout: 0

SSID Properties

SSID:

VLAN:

Interface: Radio0-802.11G

Client Authentication Settings

Methods Accepted: Open Authentication: <NO ADDITION>

Server Priorities:

EAP Authentication Servers : Use Defaults

MAC Authentication Servers : Use Defaults

Client Authenticated Key Management :

Key Management: NONE

WPA Pre-shared Key: ASCII

IDS Client MFP: Enable Client MFP on this SSID: Optional

AP Authentication

Credentials: NONE

Authentication Methods Profile: NONE

Accounting Settings

Accounting Server Priorities: Use defaults

Guest Mode/Infrastructure SSID Settings

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID: Wireless_A.T.E.I_of_Chania_0x

Set Infrastructure SSID: Wireless_A.T.E.I_of_Chania_0x

5.2.4 ΑΝΤΙΓΡΑΦΗ CONFIGURATION / ΕΠΑΝΑΦΟΡΑ CONFIGURATION

Για να εμφανίσουμε την configuration την οποία φτιάξαμε με Web Browser του BVI1 interface, αφού πάρουμε το Access Point κονσόλα εκτελούμε τα εξής :

Noc_Ap_Chania_0X>**enable**

Noc_Ap_Chania_0X#**show configuration**

Η configuration θα εμφανίζεται σταδιακά. Δημιουργούμε ένα txt αρχείο και μέσα σε αυτό αντιγράφουμε (Copy – Paste) την configuration που παίρνουμε από το Hyper Terminal. Η Διαδικασία απαιτεί προσοχή και πρέπει να πραγματοποιηθεί σταδιακά προκειμένου να αποφευχθούν τυχόν λάθη. Αφού ολοκληρώσουμε την διαδικασία αντιγραφής της configuration, Έχουμε ένα αντίγραφο που μπορούμε να επαναφέρουμε το Access Point στις **δικές μας αρχικές** ρυθμίσεις.

Αυτό γίνεται ως εξής :

Παίρνουμε το Access Point κονσόλα από το Hyper Terminal και μπαίνουμε μέσα στο cofig-terminal προκειμένου να εισάγουμε την configuration που έχουμε α-ποθηκευμένη στο txt αρχείο μας.

User Access Verification

Username: **xxxxx**

Password: **xxxxxxxxxxxx**

Noc_Ap_Chania_0X>**enable**

Noc_Ap_Chania_0X#**conf**

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Noc_Ap_Chania_0X(config)#...

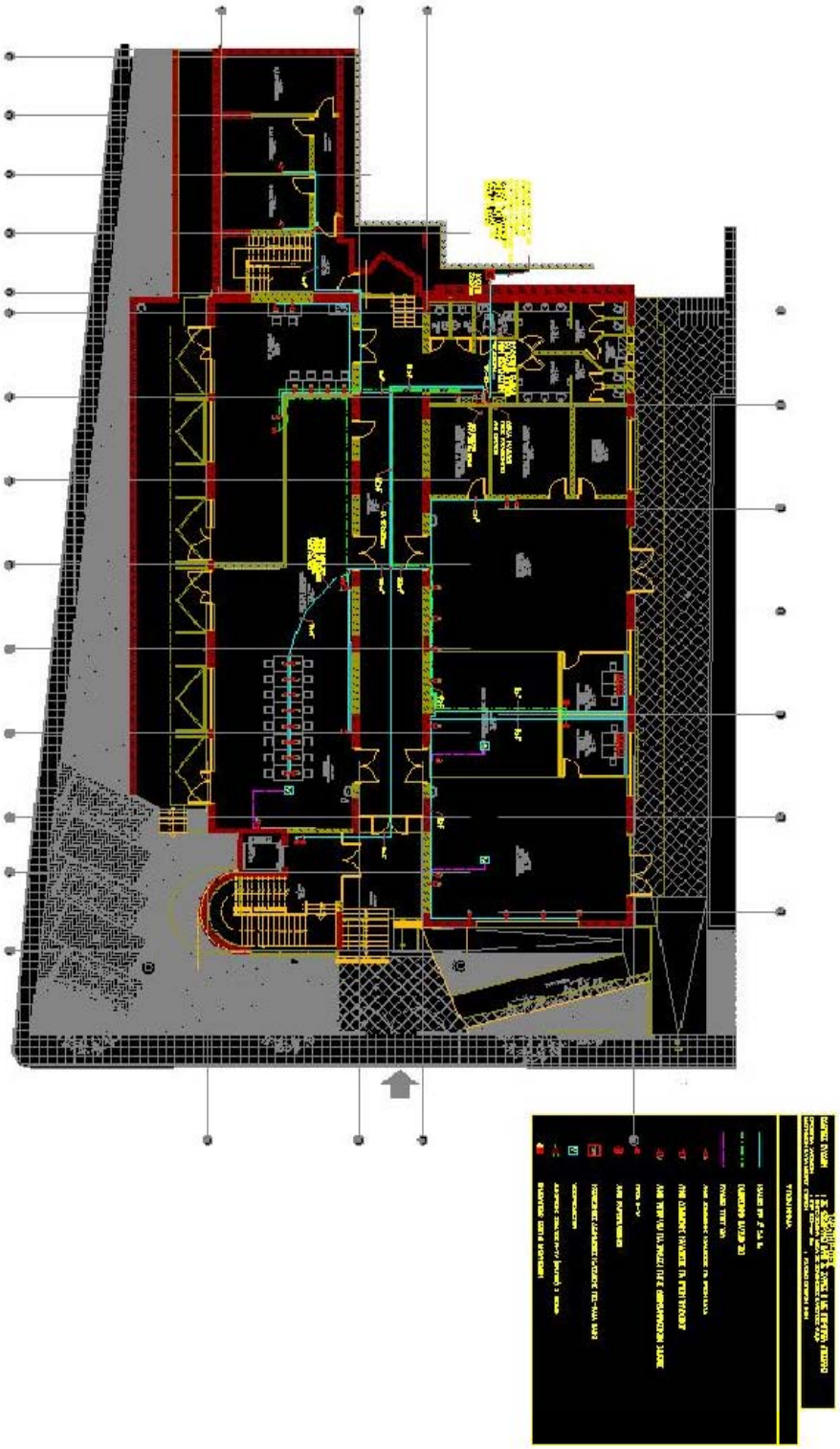
Σε αυτό το σημείο περνάμε με τη μέθοδο (Copy – Paste) την configuration.

ΠΡΟΣΟΧΗ! Δεν αντιγράφουμε όλες τις σειρές μαζί. Τις περνάμε λίγες λίγες (4-5 σειρές) για να ελέγχουμε τυχόν σφάλματα που μπορεί να προκύπτουν και να τα διορ-θώνουμε.

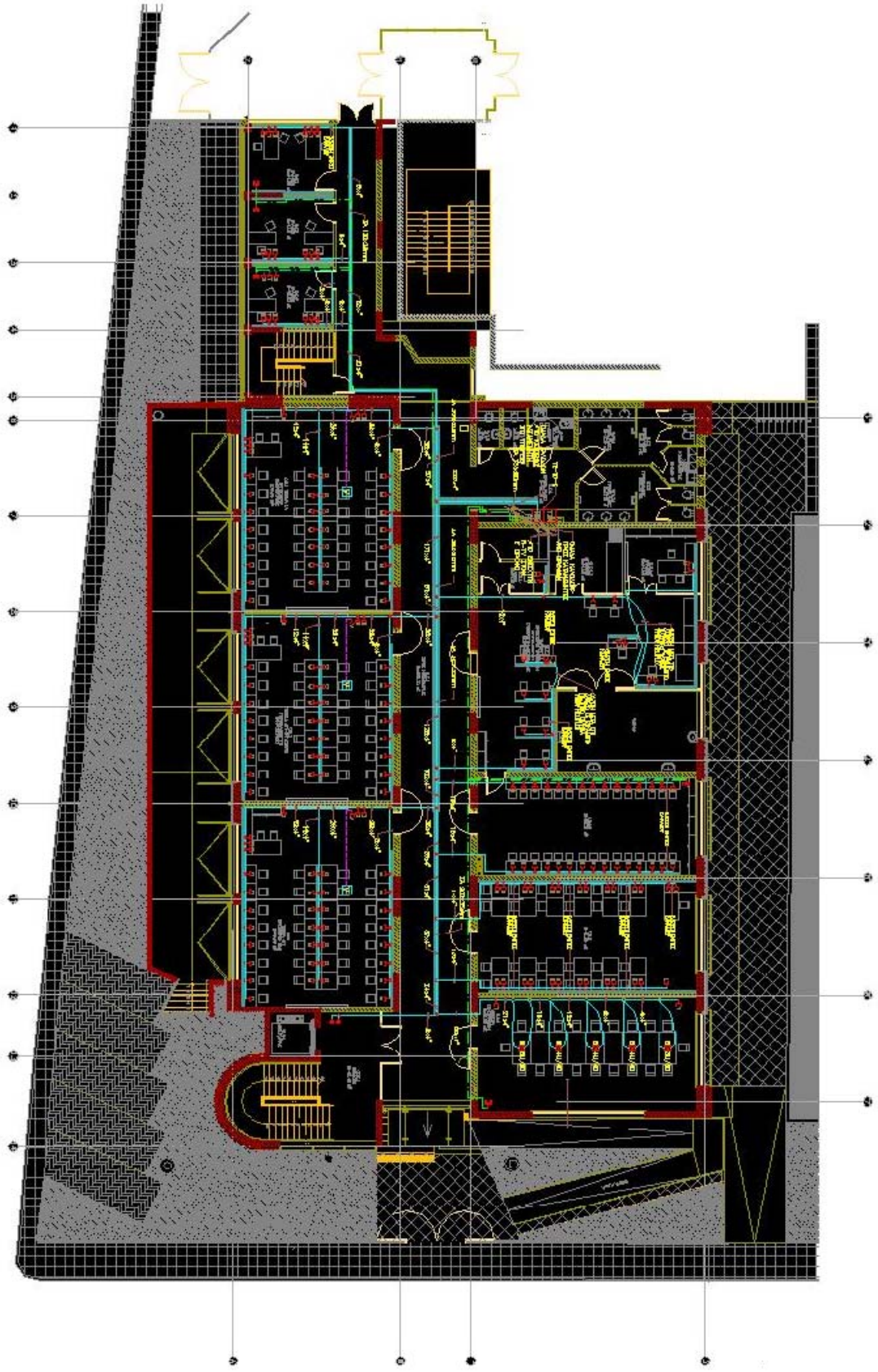
ΚΕΦΑΛΑΙΟ 6^{0}

6.1 Παρουσίαση μηχανολογικών σχεδίων (Telephony – Data) του νέου κτηρίου του ΤΕΙ Χανιών.

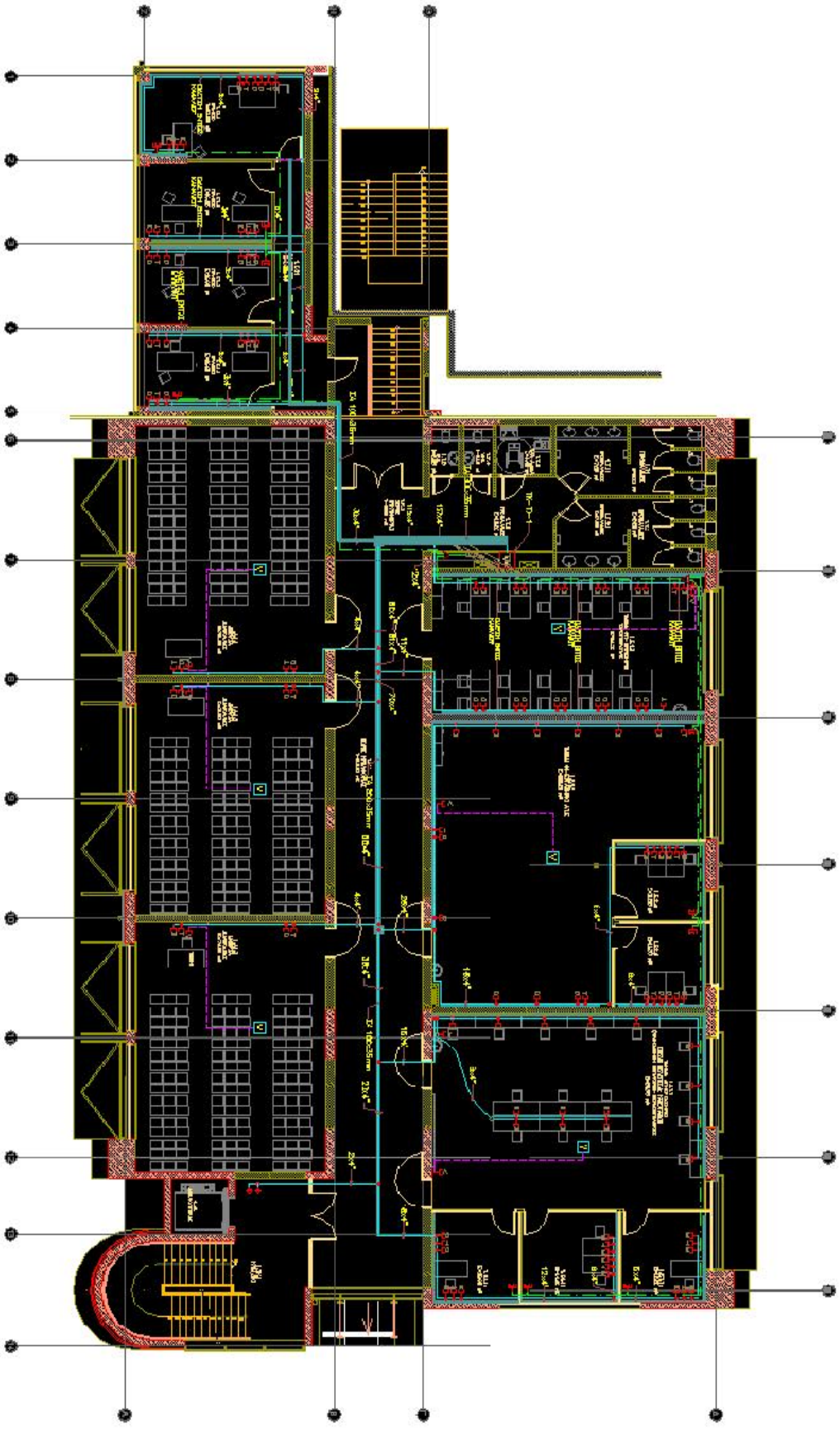
Υπόγειο



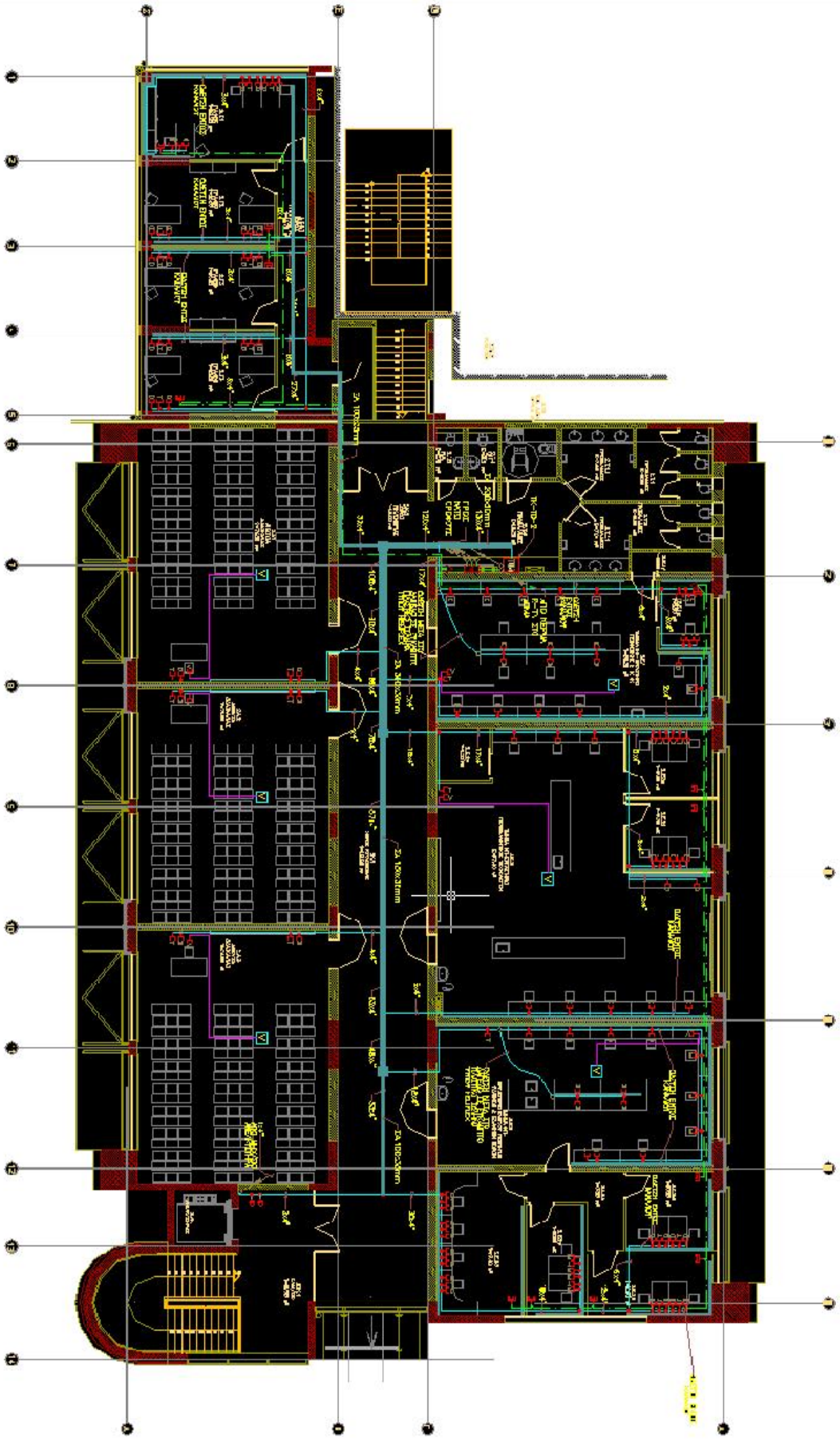
Ισόγειο



1ος όροφος



2ος όροφος



Ταράτσα